User Manual

YOYORouter

High Performance Combo Router BE5

Multi-access router with 3G HSPA, WLAN 802.11n, Ethernet, Telephony and SMS

Copyright

The contents of this publication may not be reproduced in any part or as a whole, stored, transcribed in an information retrieval system, translated into any language, or transmitted in any form or by any means, mechanical, magnetic, electronic, optical, photocopying, manual, or otherwise, without the prior written permission.

Trademarks

All products, company, brand names are trademarks or registered trademarks of their respective companies. They are used for identification purpose only. Specifications are subject to be changed without prior notice.

FCC Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against radio interference in a commercial environment. This equipment can generate, use and radiate radio frequency energy and, if not installed and used in accordance with the instructions in this manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures are necessary to correct the interference.

CE Declaration of Conformity

This equipment complies with the requirements relating to electromagnetic compatibility, EN 55022/A1 Class B.

V2.00

TABLE OF CONTENTS

COPYRIGHT 2

FCC INTERFERENCE STATEMENT 2

1. INTRODUCTION 5

1.1. Package List 5
1.2. Hardware Overview 5
1.2.1. Front Panel 5
1.3. LED indicators 6

2. GETTING STARTED 7

2.1. Operating Modes 7
2.2. Preparing YOYORouter BE5 8
2.3. Connecting to YOYORouter BE5 9
2.4. Accessing the Status & Configuration Pages 10
2.5. Setting up YOYORouter BE5 in Wireless WAN Mode 11
2.6. Setting up YOYORouter BE5 in Ethernet WAN mode 12
2.7. Setting up YOYORouter BE5 in Ethernet WAN mode with 3G Failover 13
2.8. Checking Failover to 3G 14
2.9. Wi-Fi Configuration Tips 16
2.10. Connecting to the YOYORouter using WPS 16

3. CONFIGURATION REFERENCE GUIDE 17

3.1. Using the Setup Wizard 17
3.1.1. Starting the Wizard 17
3.1.2. Configure Settings using the Wizard 18
3.2. Advanced Settings 21
3.2.1. Basic Setting Group 21
3.2.1.1. Network Setup 21
3.2.1.2. DHCP Server 31
3.2.1.3. Wireless Settings 34
3.2.1.4. Change Password 39
3.2.2. Forwarding Rules 40
3.2.2.1. Virtual Server 40
3.2.2.2. Special AP 41
3.2.2.3. Miscellaneous 42
3.2.3. Security Setting 43
3.2.3.1. Packet Filters 44
3.2.3.2. Domain Filters 46
3.2.3.3. URL Blocking 47
3.2.3.4. MAC Control 48
3.2.3.5. Miscellaneous 50
3.2.4. Advanced Settings 51
3.2.4.1. System Log 52
3.2.4.2. Dynamic DNS 53
3.2.4.3. QOS 54
3.2.4.4. SNMP 55
3.2.4.5. Routing 56
3.2.4.6. System Time 57

3.2.4.7. Scheduling 58
3.2.5. Voice 60
3.2.5.1. Missed Calls 60
3.2.5.2. Incoming Calls 60
3.2.5.3. Outgoing Calls 61
3.2.5.4. Telephone settings 61
3.2.5.5. Call Waiting 62
3.2.5.6. Speed Dial 63
3.2.6. SMS 64
3.2.6.1. Create Message 64
3.2.6.2. Inbox 65
3.2.7. Tool Box 66
3.2.7.1. System Info 67
3.2.7.2. Firmware Upgrade 68
3.2.7.3. Backup Setting 68
3.2.7.4. Reset to Default 69
3.2.7.5. Reboot 69
3.2.7.6. Miscellaneous 70

4. USING THE TELEPHONE FEATURE 71

4.1. Overview 71
4.2. Using the Telephone 71
4.2.1. To make a call 71
4.2.2. To receive a call 72
4.2.3. Admin Features 72

5. TROUBLESHOOTING 73

5.1. Basic Problems 73
5.2. Wi-Fi Problems 73
5.3. Problems with the Mobile Broadband Connection 75
5.4. Other Problems 77

APPENDIX A LICENSING INFORMATION 78

1. Introduction

Congratulations on your purchase of a YOYORouter B1. This product is specifically designed for mobile user who needs to have the Internet access beyond his home and office. It provides a complete solution for Internet surfing and broadband sharing.

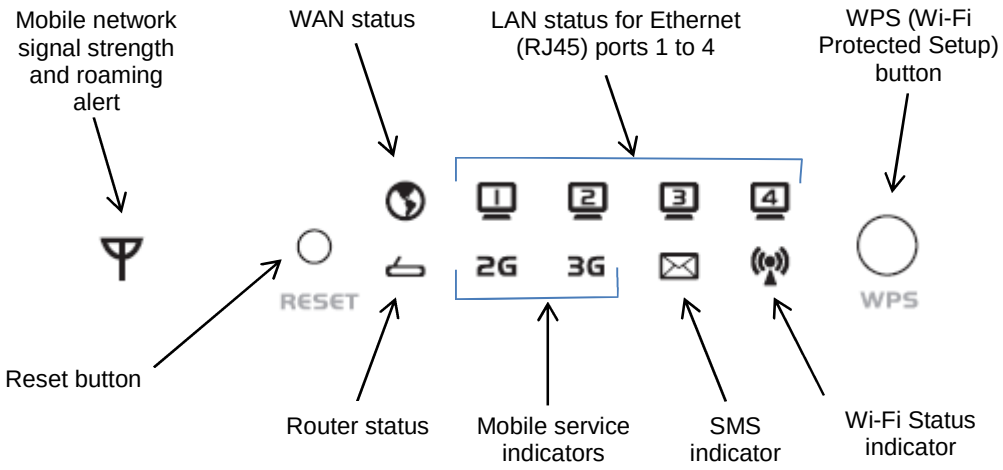
The Quick-Start Guide shows how to get up and running with the YOYORouter B1. This User Guide provides in-depth instructions to use all of the features.

1.1. Package List

Items	Description
1	YOYORouter BE5
2	Power adapter 12V 1A
3	3G Antenna
4	Quick-Start Guide
5	CD-ROM (PDF User Guide)

1.2. Hardware Overview

1.2.1. Front Panel



1.3. LED indicators

Signal Strength and Roaming Alert	
	Disconnected No signal; no SIM card; incorrect or missing PIN
	Connected, low signal
	Connecting
	Connected, medium signal
	Connected, strong signal
	Fast Flash denotes roaming

WAN Status	
	WAN Ethernet (RJ45) cable connected
	Data transfer over WAN

LAN Status	
	LAN Ethernet (RJ45) cable connected
	Data transfer over LAN port

Wi-Fi Status	
	Wi-Fi (WLAN) is on
	Data transfer over Wi-Fi
	Fast flash denotes WPS mode

SMS Indicator	
	Storage full; make space in Inbox
	Unread message(s) in Inbox

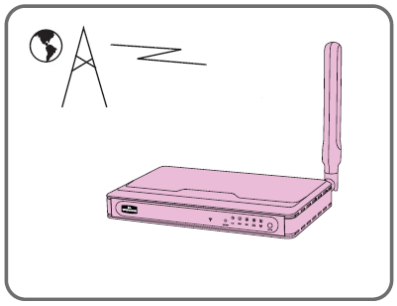
Mobile Service Indicators	
	Mobile network service is 2G (GPRS or EDGE)
	Data transfer over 2G
	Mobile network service is 3G (HSPA/HSDPA/UMTS)
	Data transfer over 3G

Router Status	
	Router operating

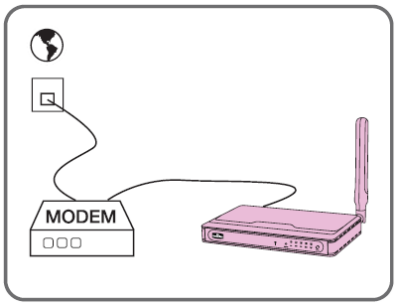
2. Getting Started

2.1. Operating Modes

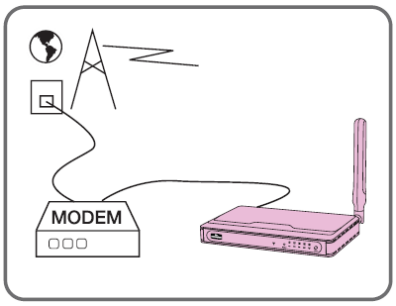
YOYORouter BE5 has three operating modes to optimally provide internet service from a cabled WAN (Wide Area Network) or the built-in Wireless WAN (3G Mobile Broadband):



Wireless WAN (Mobile Broadband) Mode
Make a Mobile Broadband connection using HSPA/HSDPA/UMTS/EDGE/GPRS and share it over Wi-Fi and with up to four devices connected using Ethernet (RJ45).



Ethernet WAN Mode
Connect to a cabled Ethernet WAN connection such as an ADSL or cable modem – share it with Wi-Fi devices and up to four devices connected using Ethernet (RJ45).



Ethernet WAN Mode with Failover
Operate in Ethernet WAN Mode and automatically switch over to Wireless WAN Mode if the cabled WAN connection fails.

In any of these modes, YOYORouter BE5 can also send and receive SMS messages and make/receive mobile phone calls via a connected telephone. (A SIM supporting these services must be plugged in).

2.2. Preparing YOYORouter BE5

Follow these steps to connect up your YOYORouter and access the configuration wizard to configure it to your needs.

1. Attach the 3G antenna
   - Locate the antenna's plug against the antenna socket on the rear panel.
   - Turn the grooved ring clockwise to secure the plug in the socket.
   - Once secured, position the antenna to point vertically upwards. This will ensure optimal reception

2. Insert the SIM card
   - **WARNING:** Always be sure to disconnect the power before inserting or removing the SIM card. Do not touch the gold contacts of the SIM Card.
   - Hold the SIM card in line with the slot (gold contacts on the underside) and insert it gently until it clicks in to place.
   - When in place, the SIM card projects from the back panel by approximately 2mm.
   - To remove the SIM, press gently inwards until you hear a click; the SIM card will then be ejected.

   Note: A SIM card is not required if the BE5 is to be used in Ethernet WAN Mode only with no phone or SMS.

3. Connect the WAN Cable
   - Plug in the Ethernet (RJ45) cable from the internet connection, for example a cable or ADSL modem.
   - Ensure this cable is connected to the WAN port as shown.
   - When used in Mobile Broadband mode, it is not necessary to connect the WAN cable.

4. Connect the Power Cable
   - Connect the cable from the power adaptor to the power inlet socket on the back panel, as shown
   - Plug the power adaptor in to a wall outlet or socket strip.
   - Turn on YOYORouter using the on-off switch next to the power connector

2.3. Connecting to YOYORouter BE5

Using Ethernet cable (easiest):

- Plug in the Ethernet cable to a LAN port and check that the corresponding LAN indicator lights up.

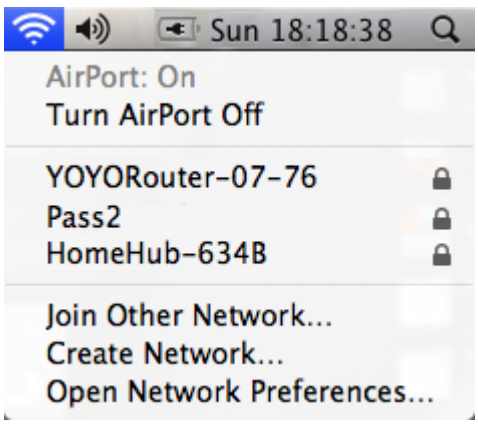
YOYORouter's Wi-Fi network has a network name (SSID) like YOYORouter-07-76. The network name and password are printed on the label on the underside of the device and on the label affixed to the carton in which it was packaged.

To connect using Wi-Fi (Microsoft Windows 7):

- Click the icon in the notification area
- Select YOYORouter's network.
- Click **Connect** and enter the Wi-Fi password when prompted.

To connect using Wi-Fi (Mac):

- Click the network icon
- Select the YOYORouter's network.
- When prompted, enter the Wi-Fi password.

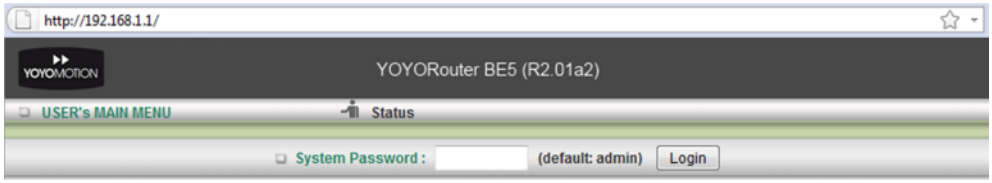


Note: since connections to YOYORouter are made using Wi-Fi and Ethernet, a wide range of devices including Linux based and mobile can connect without needing any special software or

drivers.

2.4. Accessing the Status & Configuration Pages

1. While connected, open your web browser and enter http://192.168.1.1. The YOYORouter status page is displayed.



2. To view and change settings, enter the password, default *admin*, and click **Login.**

2.5. Setting up YOYORouter BE5 in Wireless WAN Mode

1. Plug in your SIM card and switch on YOYORouter. Allow 60 seconds for network scanning.

In most cases BE5 self-configures in Wireless WAN mode using default settings. You may need to customize the settings, for example in the following cases:

- Your SIM requires a PIN Code.
- Your mobile broadband subscription requires different settings to those that YOYORouter selected by default.
- You have special mobile broadband settings, for example a private APN (Access Point Name).
- You wish to change Wi-Fi settings.

To customize settings:

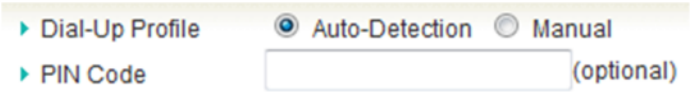
2. Connect to YOYORouter, access the status page at http://192.168.1.1 and log in.

3. Select **Wizard** and step through the Setup wizard.

- At **Select WAN Type** choose **Setup WAN Type Manually**
- Select **WAN Interface** option **Wireless WAN**
- Select **WAN Type 3G**

4. 3G Mobile Network Settings

- Connection settings are normally selected automatically from your SIM.
- Select **Dial-Up Profile** option **Manual** at the 3G step if you need to select alternative or enter special settings. Select your country and the network operator, or **Others** to enter your own settings.
- If your SIM requires a PIN code, enter it now.



5. At the end of the Wizard, click **Apply Settings**. YOYORouter restarts.

6. If you are connecting using Wi-Fi, you may need to re-make the connection in line with your new settings.

2.6. Setting up YOYORouter BE5 in Ethernet WAN mode

1. Plug in the Ethernet cable (for example from an ADSL modem) to the WAN port and switch on YOYORouter.

2. Connect to YOYORouter, access the status page at http://192.168.1.1 and log in.

3. Select **Wizard** and step through the Setup wizard.

4. At the step **Select WAN Type**
- Choose **Setup WAN Type Manually.**
- Select **WAN Interface** type **Ethernet WAN.**
- Select the required **WAN Type.**
- Enter the further information requested, as applicable. See Configuration Reference section in the User Guide for more information.

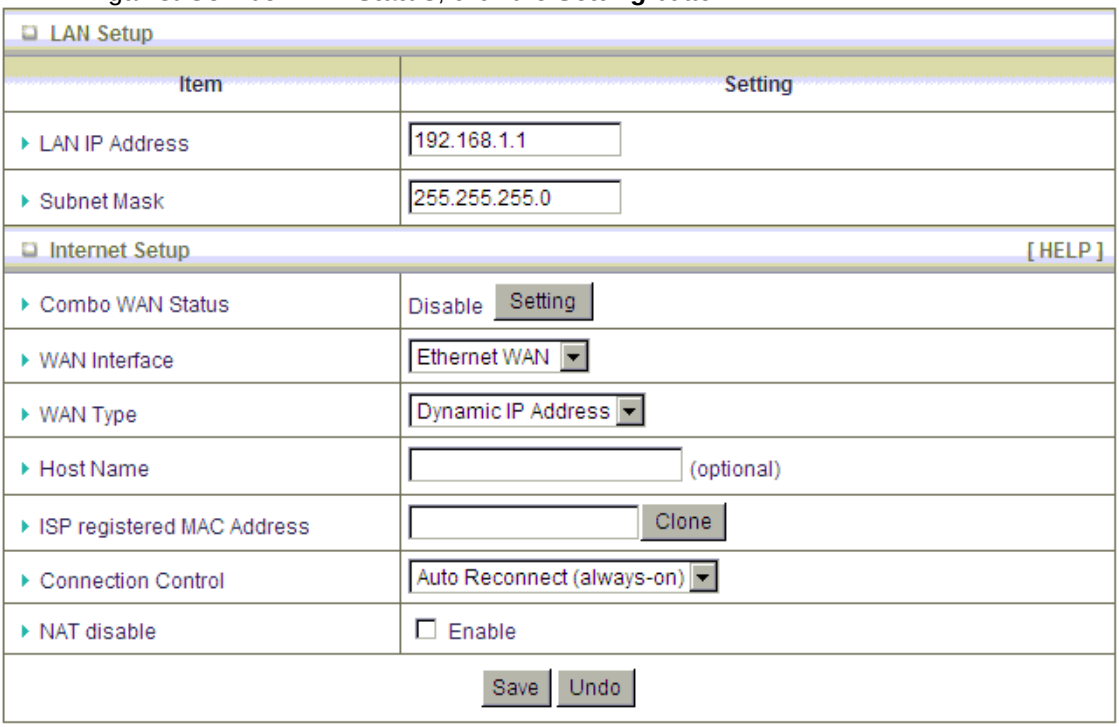
5. At the end of the Wizard, click **Apply Settings**. YOYORouter restarts.

6. If you are connecting using Wi-Fi, you may need to re-make the connection in line with your new settings.

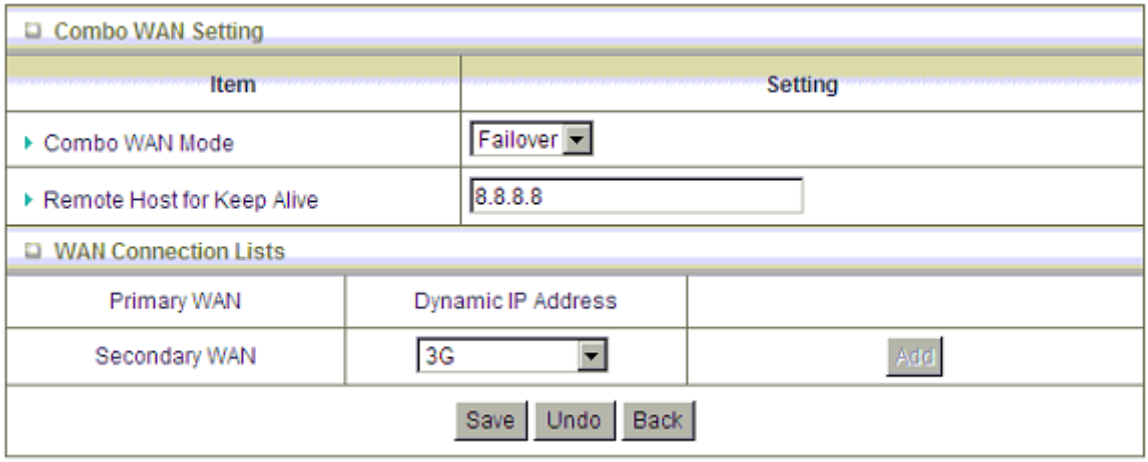
2.7. Setting up YOYORouter BE5 in Ethernet WAN mode with 3G Failover

Configure YOYORouter BE5 in Ethernet WAN mode and test the connection.
To add failover to 3G Wireless WAN, ensure that your SIM Card is inserted and the Ethernet WAN is
connected then follow these steps:

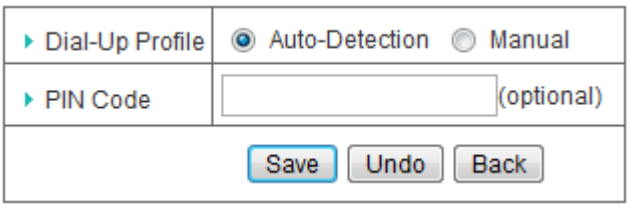
1. Log in.
2. Select **Advanced** then **Network Setup**.
3. Make sure that **Connection Control** is set to **Auto Reconnect (always-on).**
4. Against **Combo WAN Status**, click the **Setting** button.



5. Set **Combo WAN Mode** to **Failover**.
6. Enter an IP address in **Remote Host for Keep Alive** that YOYORouter can ping to check the connectivity. This can be numeric, e.g. 8.8.8.8 or text, e.g. www.google.com.
7. Your Ethernet WAN connection is shown as **primary WAN**. To add the 3G WAN as failover, click the Add button against **Secondary WAN** and select **3G** in the drop-down box.



8. Click the **Save** button.
9. The Dial-Up Profile (connection settings) for 3G mobile broadband are now displayed.



- Select **Auto-Detection** for automatic configuration based on your SIM card (recommended).
- Select **Manual** if you need to select alternative or enter special settings. Select your country and the network operator, or **Others** to enter your own settings.
- If your SIM requires a PIN code, enter it now.

10. Click the **Save** button then click **OK** to reboot YOYORouter.

2.8. Checking Failover to 3G

1. Check that YOYORouter is normally connected to the Ethernet WAN connection
   - **System Status** shows Ethernet WAN connection details.
   - **Failover Status** shows zeroed IP addresses and blank **Connection Time**
   - **Wireless Modem Link Status** indicates **Disconnected**.

System Status [HELP]

Item	WAN Status	Sidenote
Remaining Lease Time	00:31:25	Renew
IP Address	81.216.71.59	Release
Subnet Mask	255.255.255.128	
Gateway	81.216.71.1	
Domain Name Server	213.50.29.170 , 0.0.0.0	

Failover status

Item	Status	Sidenote
IP Address	0.0.0.0	3G
Subnet Mask	0.0.0.0	
Gateway	0.0.0.0	
Domain Name Server	0.0.0.0 , 0.0.0.0	
Connection Time	-	

Wireless Modem Information

Item	Status	Sidenote
Card Info	HSPA USB MODEM	
Link Status	Disconnected.	
Signal Strength	54%	
Network Name	Telenor SE	
Network Type	HSUPA	

2. Unplug the Ethernet cable from the WAN port and check that Failover occurs:
   - **System Status** shows blank Remaining Lease Time and zeroed IP addresses
   - **Failover Status** shows 3G connection information (IP numbers) and **Connection Time.**
   - **Wireless Modem Link Status** indicates **Connected.**

System Status [HELP]

Item	WAN Status	Sidenote
Remaining Lease Time	-	Renew
IP Address	0.0.0.0	
Subnet Mask	0.0.0.0	
Gateway	0.0.0.0	
Domain Name Server	0.0.0.0 , 0.0.0.0	

Failover status

Item	Status	Sidenote
IP Address	31.75.175.245	3G
Subnet Mask	255.255.255.255	
Gateway	10.64.64.64	
Domain Name Server	109.249.185.224 , 109.249.186.32	
Connection Time	00:00:14	

Wireless Modem Information

Item	Status	Sidenote
Card Info	HSPA USB MODEM	
Link Status	Connected.	
Signal Strength	45%	
Network Name	Telenor SE	
Network Type	HSUPA	

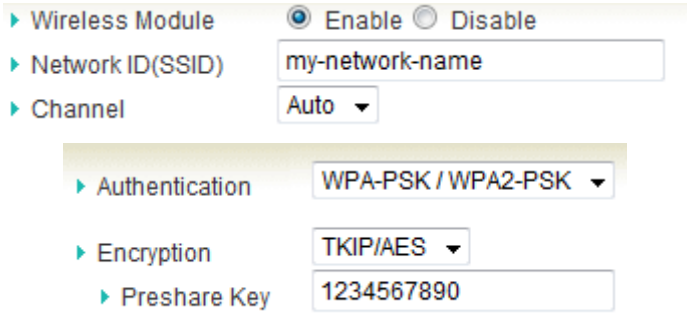
3. Re-connect the cabled WAN and check that service reverts to the WAN connection.

2.9. Wi-Fi Configuration Tips

YOYORouter is pre-configured with a default Wi-Fi network name (SSID) and password. The network name and password are printed on the label on the underside of the device and on the label affixed to the carton in which it was packaged. Security is set to WPA-PSK(TKIP) and WPA2-PSK(AES) – devices may connect using either of these.

In the Configuration Wizard you can:

- Change the Network ID (SSID) to a name of your own choice.
- Manually select a frequency channel. (Default **Auto** tries to find a channel with low interference).
- Change the Authentication and Encryption settings if required.
- Set your own network password in **Preshare Key** (recommended).



2.10. Connecting to the YOYORouter using WPS

Wi-Fi Protected Setup, WPS, is a simple way to connect to the YOYORouter without needing to give the new user the Pre-Shared Key (password). Pushbutton mode provides the simplest possible configuration:

1. Locate the WPS pushbutton on the device that you wish to connect to the router. This may be a physical button or a clickable pushbutton in the software provided with the device.
2. Press and hold the YOYORouter WPS button for 5 seconds. The Wi-Fi indicator will flash rapidly ,.
3. Bring the device near to the YOYORouter and press the WPS button on the device. You must do this inside two minutes, while the Wi-Fi indicator flashes rapidly. The GUI on the connecting device will confirm the connection.

PIN Mode is also supported – please see the User Guide for details.

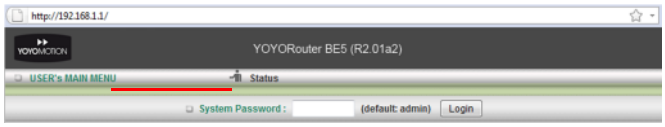
3. Configuration Reference Guide

3.1. Using the Setup Wizard

3.1.1. Starting the Wizard

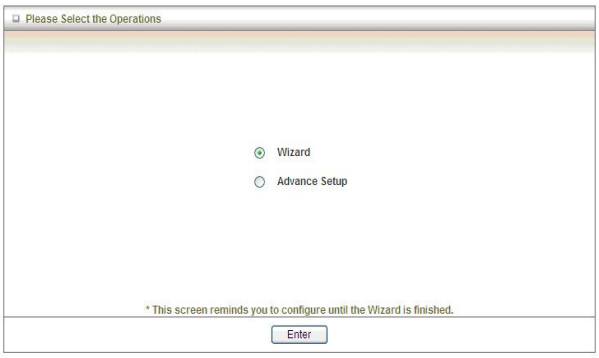
Connect to YOYORouter.

Open your browser and type in the IP Address (http://192.168.1.1)

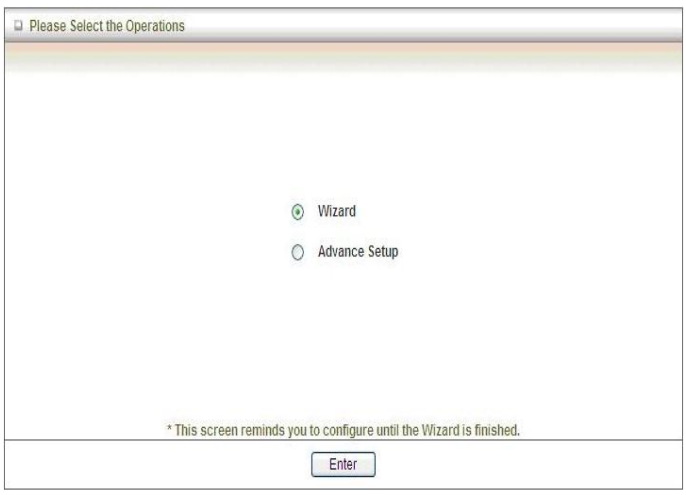


Please type “admin” in the Password and click the **Login** button.

Select your language.


Please Select the Operations
Wizard
Advance Setup
* This screen reminds you to configure until the Wizard is finished.
Enter

Select “Wizard” for basic settings with simple way.


Please Select the Operations
Wizard
Advance Setup
* This screen reminds you to configure until the Wizard is finished.
Enter

Press “Next” to start the Setup Wizard.

Setup Wizard
[EXIT]
Setup Wizard will guide you through a basic configuration procedure step by step.
Step 1. Setup Login Password.
Step 2. WAN Setup.
Step 3. Wireless Setup.
Step 4. Summary.
Step 5. Finish.
< Back
[Start > Password > Time > WAN > Wireless > Summary > Finish!]
Next >

3.1.2. Configure Settings using the Wizard

Step 1.
Change System Password.

Set up your system password.
(Default：admin)

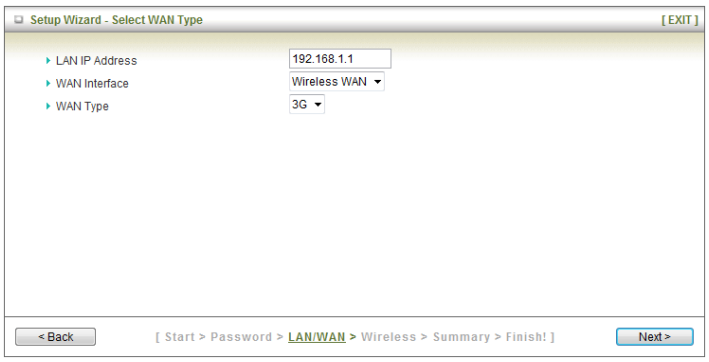
Setup Wizard - Setup Login Password
[EXIT]
Old Password
New Password
Reconfirm
< Back
[Start > Password > Time > WAN > Wireless > Summary > Finish!]
Next >

Step 2a.
Select Wan Type.
Auto Detecting or Setup Manually

Auto-detect looks for Internet over WAN first. If no connection is detected, 3G is set.

Setup Wizard - Select WAN Type
[EXIT]
Auto Detecting WAN Type
Setup WAN Type Manually
< Back
[Start > Password > Time > LAN/WAN > Wireless > Summary > Finish!]
Next >

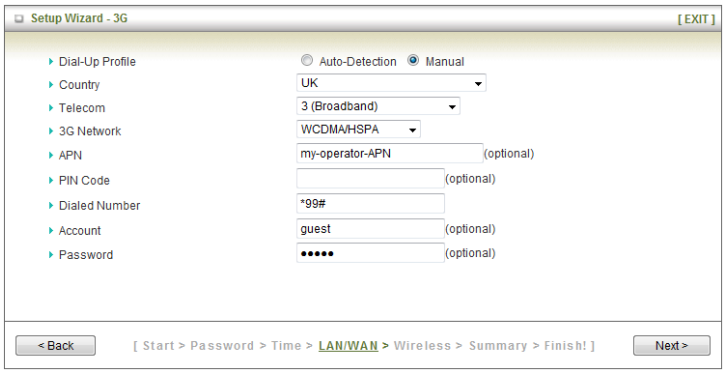
Step 2b.
Select LAN IP Address and Wan Type.



Step 2c.

3G WAN type
Select “Auto Detection” Dial-up Profile, and the Utility will try to detect and configure the required Mobile Broadband service settings automatically. Or you can select “Manual” and select your country and mobile operator. If you have special settings, for example for a private company, select your country and then **Others.**

If your SIM card requires a PIN Code, enter it, otherwise leave blank.



Step 3a.

Set up your Wireless Network.

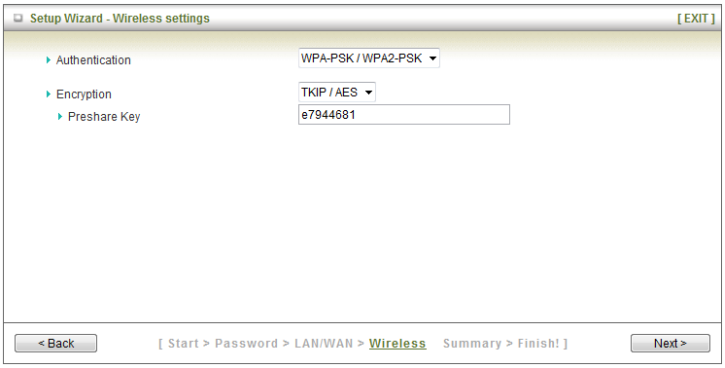
Set up your Wi-Fi network name (SSID).

Channel **Auto** (default enables the router to identify the best channel. If you wish to manually select the channel, typically 1, 6 or 11, pick it in the drop-down menu.

Step 3b.

Set up Wireless Security.

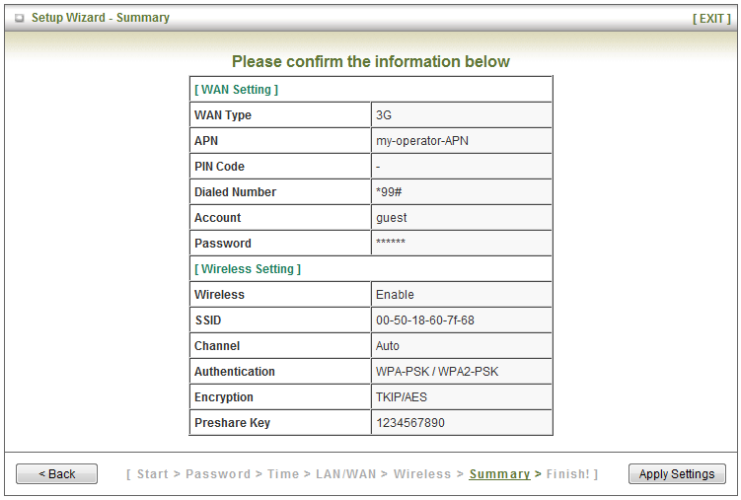
We recommend WPA-PSK / WPA2-PSK security. The settings shown provide widest compatibility.You can set your own password in **Preshare Key**.



Step 4.

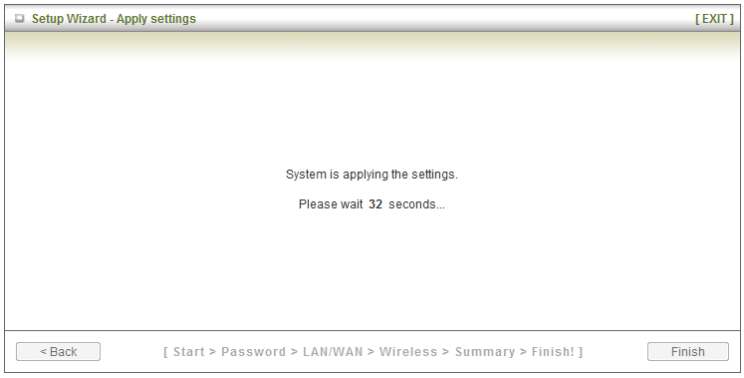
The settings you have selected are summarized. Click **Apply Settings** to confirm them.

The wizard counts down the time it takes while YOYORouter re-starts.



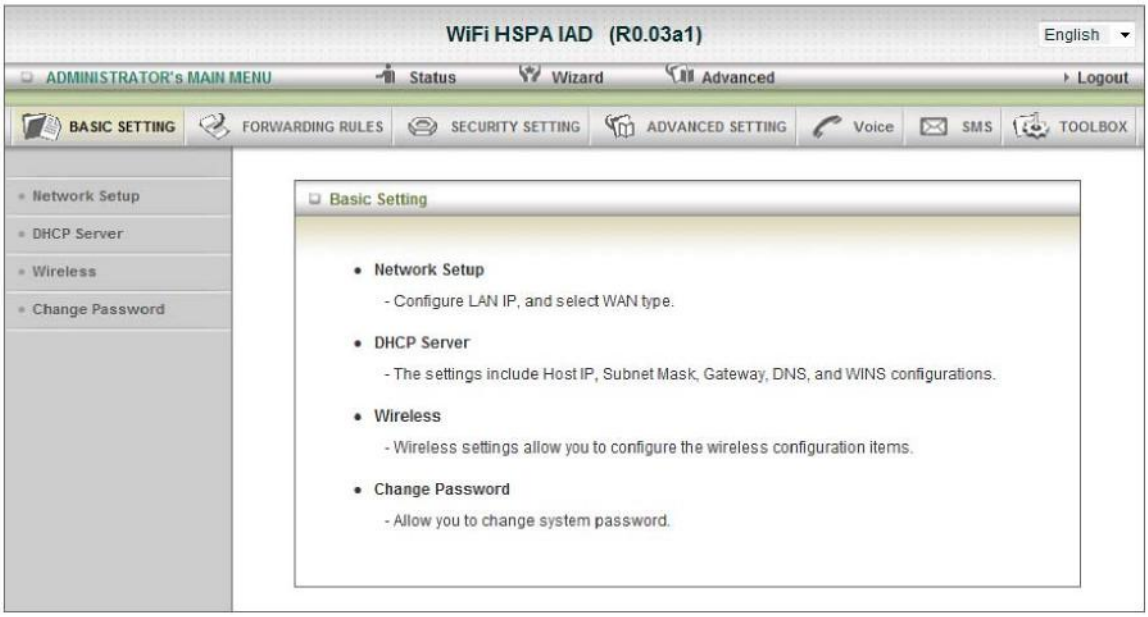
Step 5.

Click Finish to close the Wizard.
Note: The router has already restarted.


Setup Wizard - Apply settings
[EXIT]
System is applying the settings.
Please wait 32 seconds...
< Back
[Start > Password > LAN/WAN > Wireless > Summary > Finish!]
Finish

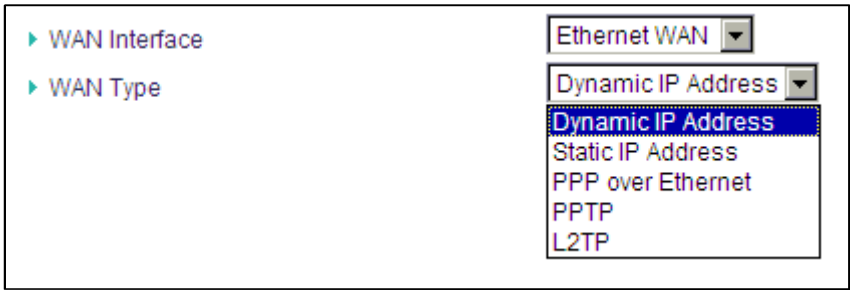
3.2. Advanced Settings

3.2.1. Basic Setting Group



3.2.1.1. Network Setup

1. **LAN IP Address:** the local IP address of this device. The computers on your network
   must use the LAN IP address of your product as their Default Gateway. You can change it if necessary.
2. **Subnet Mask: insert 255.255.255.0**
3. **Combo WAN Status:** Used to define the failover Internet source (e.g. 3G)
4. **WAN Interface:** Select Ethernet WAN or Wireless WAN to continue.
5. **WAN Type**: WAN connection type of your ISP. You can click WAN Type Combo button to choose a correct one from the following options:



A. WAN Type: Dynamic IP Address

LAN Setup

Item	Setting
LAN IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Internet Setup	[HELP]
Combo WAN Status	Disable Setting
WAN Interface	Ethernet WAN
WAN Type	Dynamic IP Address
Host Name	(optional)
ISP registered MAC Address	Clone
Connection Control	Connect-on-Demand
NAT disable	Enable

Save Undo

1. Combo WAN Status: Used to define the failover Internet source (e.g. 3G)
2. Host Name: optional, required by some ISPs, for example, @Home.
3. ISP register MAC address: You can change the WAN port MAC address, it is your ISP assigned to you.
4. Connection Control: There are 3 modes to select:

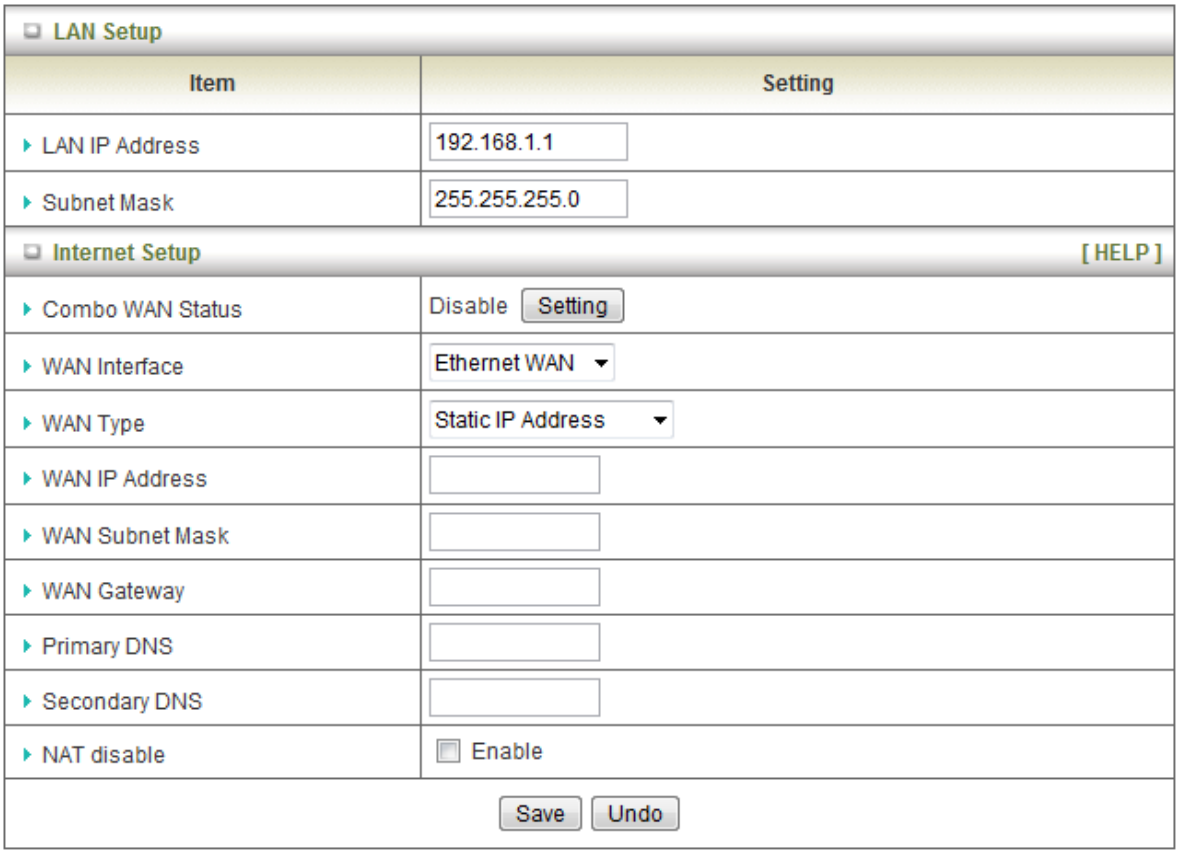
   Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.

   Auto Reconnect (Always-on): The device connects when power is switched on and remains connected.

   Manually: The device will not make the link until someone clicks the connect-button in the Status-page.

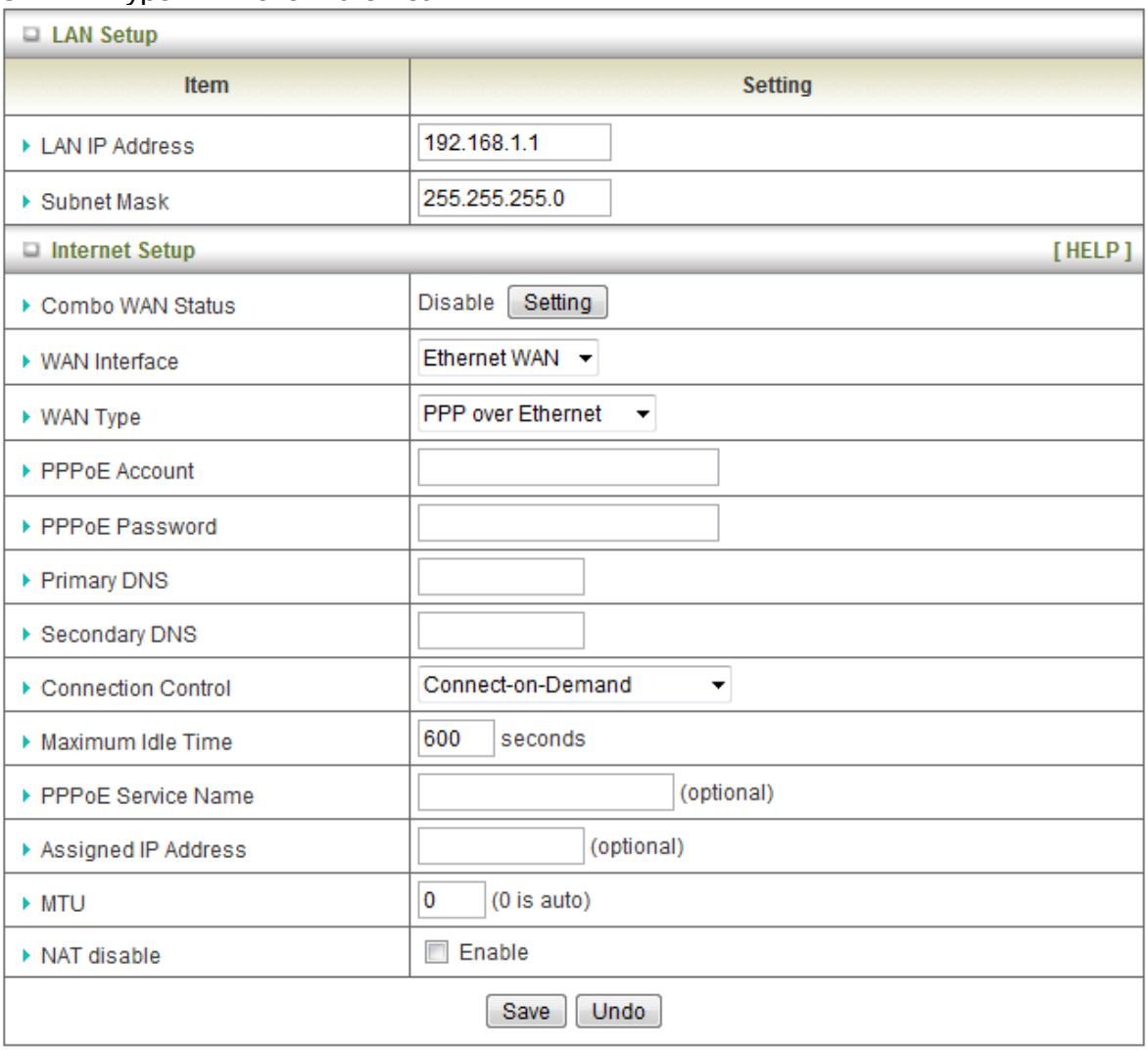
5. NAT disable**:** the option bridges data form WAN port to LAN port.

B. WAN Type: Static IP Address:



WAN IP Address, Subnet Mask, Gateway, Primary and Secondary DNS: enter the proper setting provided by your ISP.

C. WAN Type: PPP over Ethernet



1. Combo WAN Status: Used to define the failover Internet source (e.g. 3G)
2. PPPoE Account and Password: the account and password your ISP assigned to you. For security, this field appears blank. If you don't want to change the password, leave it empty.
3. Primary DNS/ Secondary DNS: This feature allows you to assign a Primary/Secondary DNS Server, contact to your ISP to get it.
4. Connection Control: There are 3 modes to select:

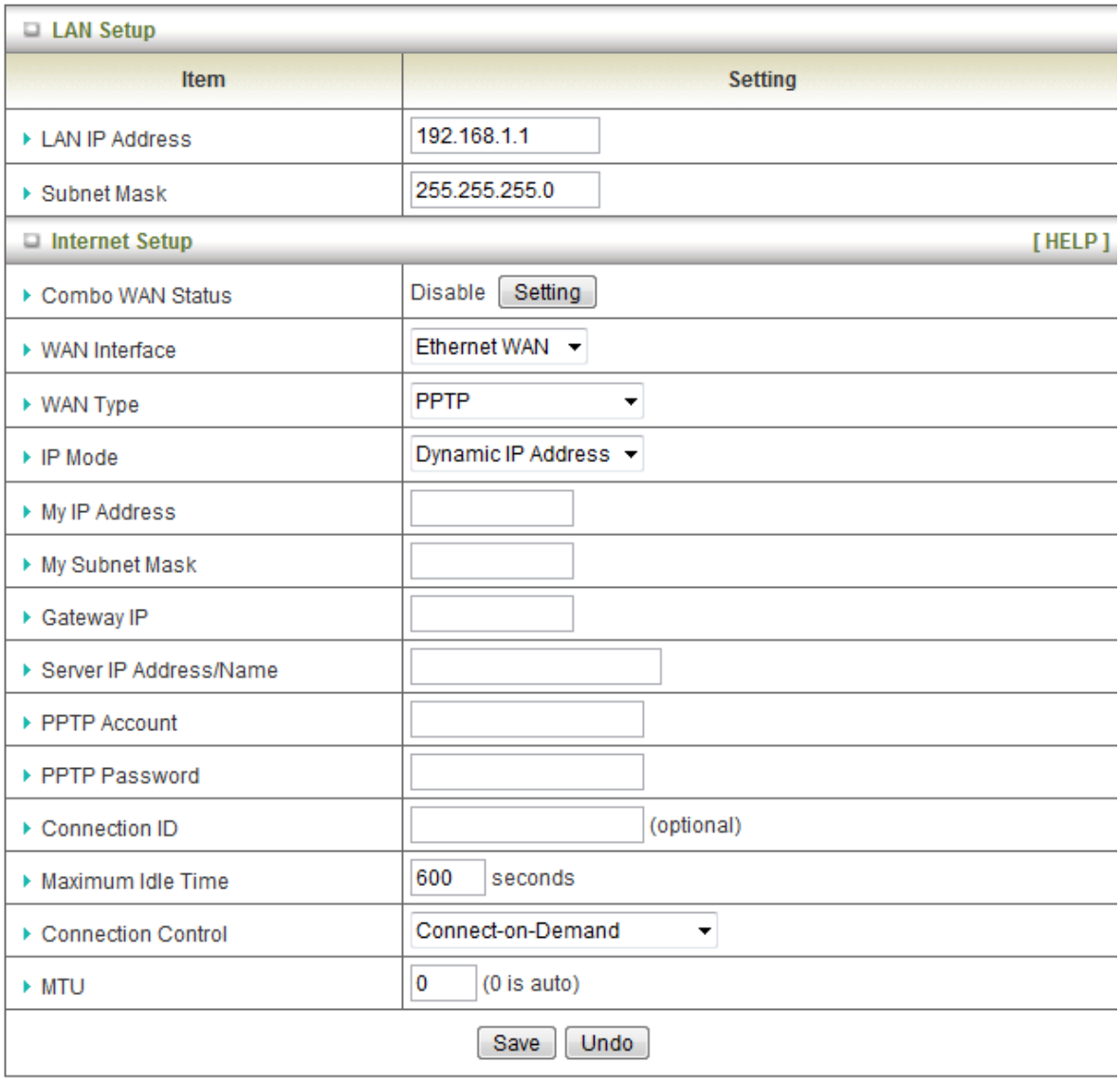
   Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.

   Auto Reconnect (Always-on): The device connects when power is switched on and remains connected.

   Manually: The device will not make the link until someone clicks the connect-button in the Status-page.
5. Maximum Idle Time: the amount of time of inactivity before disconnecting your PPPoE session. Set it to zero or enable Auto-reconnect to disable this feature.

6. PPPoE Service Name: optional. Input the service name if your ISP requires it. Otherwise, leave it blank.
7. Assigned IP address: Optional, Input the IP address you want. Usually, leave it blank.
8. Maximum Transmission Unit (MTU): Most ISP offers MTU value to users. The default MTU value is 0(auto).
9. NAT disable: the option bridges data form WAN port to LAN port

D. WAN Type: PPTP



First, please check your ISP assigned and select the IP Mode - Static IP Address or Dynamic IP Address. For example: Use Static, the private IP address, subnet mask and Gateway are your ISP assigned to you.

1. Combo WAN Status: Used to define the failover Internet source (e.g. 3G)
2. My IP Address, My Subnet Mask and WAN Gateway IP: the private IP address, subnet mask and Gateway IP your ISP assigned to you.

3. Server IP Address/Name: the IP address or URL of the PPTP server.
4. PPTP Account and Password: the account and password your ISP assigned to you. If you don't want to change the password, keep it empty.
5. Connection ID: optional. Input the connection ID if your ISP requires it.
6. Maximum Idle Time: the time of no activity to disconnect your PPTP session. Set it to zero or enable “Auto-reconnect” to disable this feature. If Auto-reconnect is enabled, this product will connect with ISP automatically, after system is restarted or connection is dropped.
7. Connection Control: There are 3 modes to select:

   Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.

   Auto Reconnect (Always-on): The device connects when power is switched on and remains connected.

   Manually: The device will not make the link until someone clicks the connect-button in the Status-page.

8. Maximum Transmission Unit (MTU): Most ISP offers MTU value to users. The default MTU value is 0(auto).

E. WAN Type: L2TP

LAN Setup	
Item	**Setting**
LAN IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Internet Setup	[HELP]
Combo WAN Status	Disable Setting
WAN Interface	Ethernet WAN
WAN Type	L2TP
IP Mode	Dynamic IP Address
IP Address	
Subnet Mask	
WAN Gateway IP	
Server IP Address/Name	
L2TP Account	
L2TP Password	
Maximum Idle Time	600 seconds
Connection Control	Connect-on-Demand
MTU	0 (0 is auto)
Save Undo	

First, please check your ISP assigned and select the IP Mode - Static IP Address or Dynamic IP Address. For example: Use Static, the private IP address, subnet mask and Gateway are your ISP assigned to you.

1. Combo WAN Status: Used to define the failover Internet source (e.g. 3G)
2. IP Address, Subnet Mask and WAN Gateway IP: the private IP address, subnet mask and Gateway IP your ISP assigned to you.
3. Server IP Address/Name: the IP address or URL of the PPTP server.
4. L2TP Account and Password: the account and password your ISP assigned to you. If you don't want to change the password, keep it empty.
5. Maximum Idle Time: the time of no activity to disconnect your L2TP session. Set it to zero or enable “Auto-reconnect” to disable this feature. If Auto-reconnect is enabled, this product will connect with ISP automatically, after system is restarted or connection is dropped.

6. Connection Control: There are 3 modes to select:
   Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.

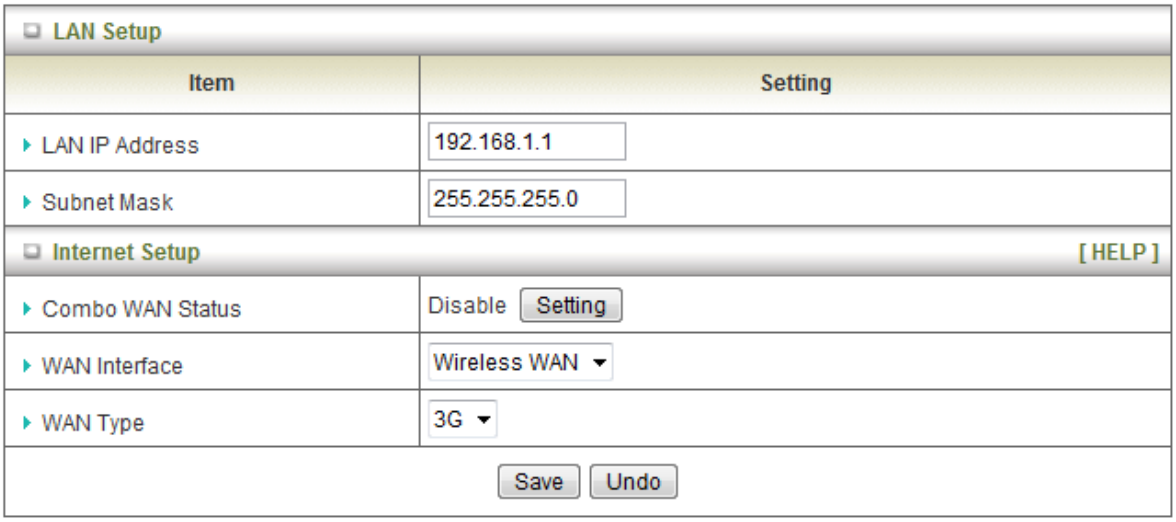
   Auto Reconnect (Always-on): The device connects when power is switched on and remains connected.

   Manually: The device will not make the link until someone clicks the connect-button in the Status-page.

7. Maximum Transmission Unit (MTU): Most ISP offers MTU value to users. The default MTU value is 0(auto).

F. WAN Type: Wireless WAN: 3G

Select **Wireless WAN** and **3G**



Against **Dial-Up Profile**:

- Select **Auto-Detection** for automatic configuration based on your SIM card (recommended).
- Select **Manual** if you need to select alternative or enter special settings. Select your country and the network operator, or **Others** to enter your own settings.
- If your SIM requires a PIN code, enter it now.

To set up manually:

1. Country: select your country.
2. Telecom: select your network operator.
3. 3G Network: always WCDMA/HSPA.
4. APN: Enter the APN for your network operator subscription. (Sometimes it is left blank)
5. Pin Code: Enter the Pin Code for your SIM card (Optional)
6. Dial-Number: *99# This field should not be altered except when required by your service provider.
7. Account: Enter the new User Name associated with the APN, you can contact to your mobile operator to get it. (Optional)
8. Password: Enter the new Password associated with the APN, you can contact to your mobile operator to get it. (Optional)
9. Authentication: Choose your authentication.
10. Primary DNS: This feature allows you to assign a Primary DNS Server, contact to your ISP to get it.
11. Secondary DNS: This feature allows you to assign a Secondary DNS Server, you can contact to your ISP to get it.
12. Connection Control: select your connection control
13. Keep Alive: you can diagnose your connection by it.

LAN Setup	
Item	**Setting**
LAN IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Internet Setup	[HELP]
Combo WAN Status	Disable [Setting]
WAN Interface	Wireless WAN
WAN Type	3G
Dial-Up Profile	○ Auto-Detection ◉ Manual
Country	
Telecom	
3G Network	WCDMA/HSPA
APN	orangeinternet (optional)
PIN Code	(optional)
Dialed Number	*99#
Account	(optional)
Password	(optional)
Authentication	◉ Auto ○ PAP ○ CHAP
Primary DNS	(optional)
Secondary DNS	(optional)
Prefer Service Mode	Auto Mode
Connection Control	Auto Reconnect (always-on)
Allowed Connection Time	◉ Always ○ By Schedule
Keep Alive	◉ Disable ○ LCP Echo Request Interval 10 seconds Max Failure Time 3 times ○ Ping Remote Host Host IP Interval 60 seconds
Roaming	☐ Enable
NAT disable	☐ Enable
[Save] [Undo]	

3.2.1.2. DHCP Server

Press **"More>>",**

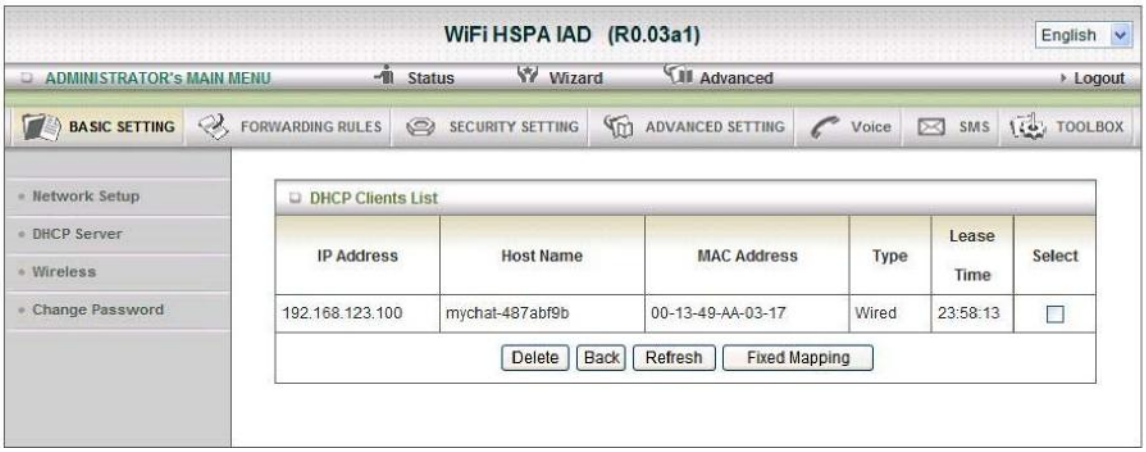
1. **DHCP Server:** Choose either **Disable** or **Enable**
2. **Lease Time:** DHCP lease time to the DHCP client
3. **IP Pool Starting/Ending Address:** Whenever there is a request, the DHCP server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting / ending address of the IP address pool
4. **Domain Name:** Optional, this information will be passed to the client
5. **Primary DNS/Secondary DNS:** Optional, This feature allows you to assign a DNS Servers
6. **Primary WINS/Secondary WINS:** Optional, this feature allows you to assign a WINS Servers

7. Gateway: Optional, Gateway Address would be the IP address of an alternate Gateway. This function enables you to assign another gateway to your PC, when DHCP server offers an IP to your PC.

Click on "Save" to store your setting or click "Undo" to give up

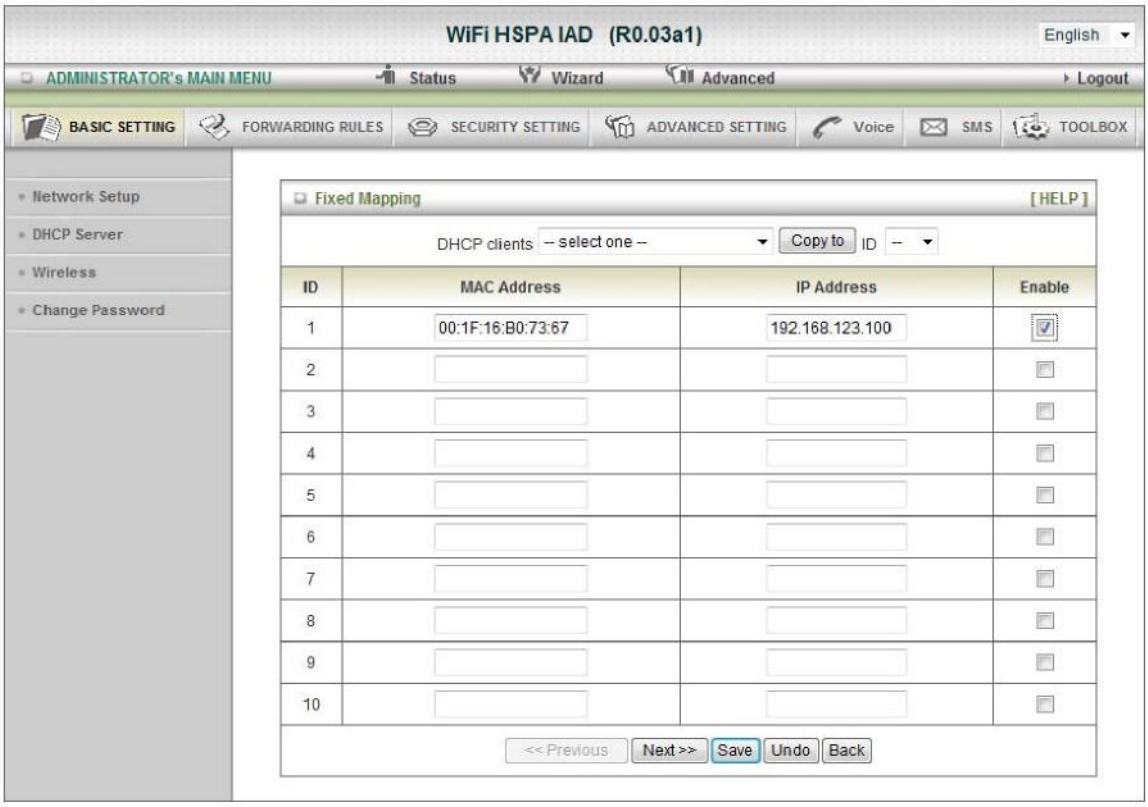
DHCP Clients List

The list of DHCP clients shows here.



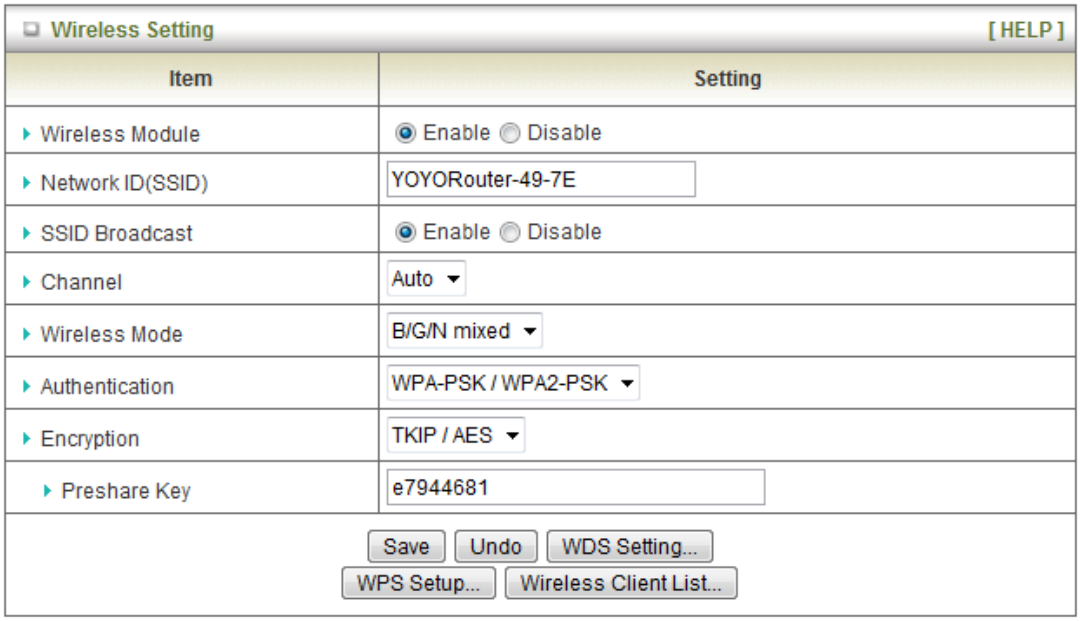
DHCP Fixed Mapping

The DHCP Server will reserve the special IP for special MAC address, shows below.



3.2.1.3. Wireless Settings

Wireless settings allow you to set the wireless configuration items.



1. **Wireless Module:** The user can enable or disable wireless function
2. **Network ID(SSID):** Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this product and other Access Points that have the same Network ID. (The factory setting is “default”)
3. **SSID Broadcast:** The router will broadcast beacons that have some information, including ssid so that wireless clients can know how many AP devices by scanning function in the network. Therefore, this function is disabled; the wireless clients can not find the device from beacons.
4. **Channel:** The radio channel number. The permissible channels depend on the Regulatory Domain.

   The factory setting is channel 11.
5. **Wireless Mode:** Choose B/G Mixed, B only, G only, N only, G/N Mixed or B/G/N mixed. The factory default setting is B/G/N mixed.
6. **Authentication mode:** You may select from nine kinds of authentication to secure your wireless network: Open, Shared, Auto, WPA-PSK, WPA, WPA2-PSK, WPA2, WPA-PSK/WPA2-PSK, WPA /WPA2.

Open

Open system authentication simply consists of two communications. The first is an authentication request by the client that contains the station ID (typically the MAC address). This is followed by an authentication response from the AP/router containing a

success or failure message. An example of when a failure may occur is if the client's MAC address is explicitly excluded in the AP/router configuration.

Shared

Shared key authentication relies on the fact that both stations taking part in the authentication process have the same "shared" key or passphrase. The shared key is manually set on both the client station and the AP/router. Three types of shared key authentication are available today for home or small office WLAN environments.

Auto

The AP will Select the Open or Shared by the client's request automatically.

WPA-PSK

Select Encryption and Pre-share Key Mode

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits. If you select ASCII, the length of pre-share key is from 8 to 63.

Fill in the key, Ex 12345678

WPA

Check Box was used to switch the function of the WPA. When the WPA function is enabled, the Wireless user must **authenticate** to this router first to use the Network service. RADIUS Server IP address or the 802.1X server's domain-name.

Select Encryption and RADIUS Shared Key

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits If you select ASCII, the length of pre-share key is from 8 to 63.

Key value shared by the RADIUS server and this router. This key value is consistent with the key value in the RADIUS server.

WPA-PSK2

WPA-PSK2 user AES and TKIP for Same the encryption, the others are same the WPA-PSK.

WPA2

WPA2 add uses AES and TKIP for encryption, the others are same the WPA.

WPA-PSK/WPA-PSK2

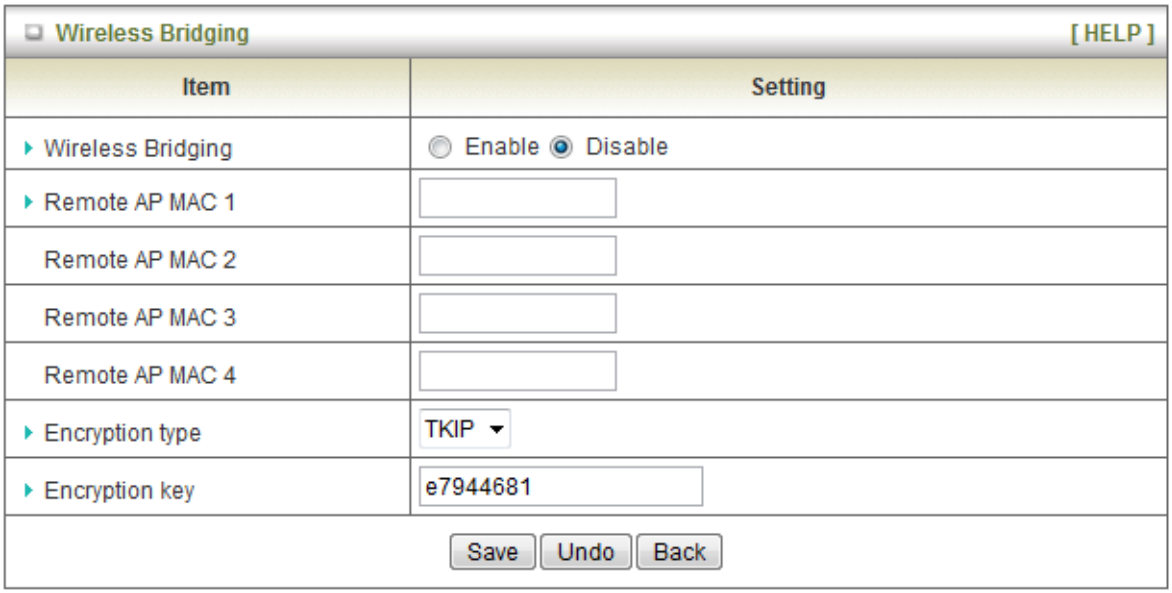
Another encryption options for WPA-PSK-TKIP and WPA-PSK2-AES, the others are same the WPA-PSK.

WPA/WPA2

Another encryption options for WPA-TKIP and WPA2-AES, the others are same the WPA.

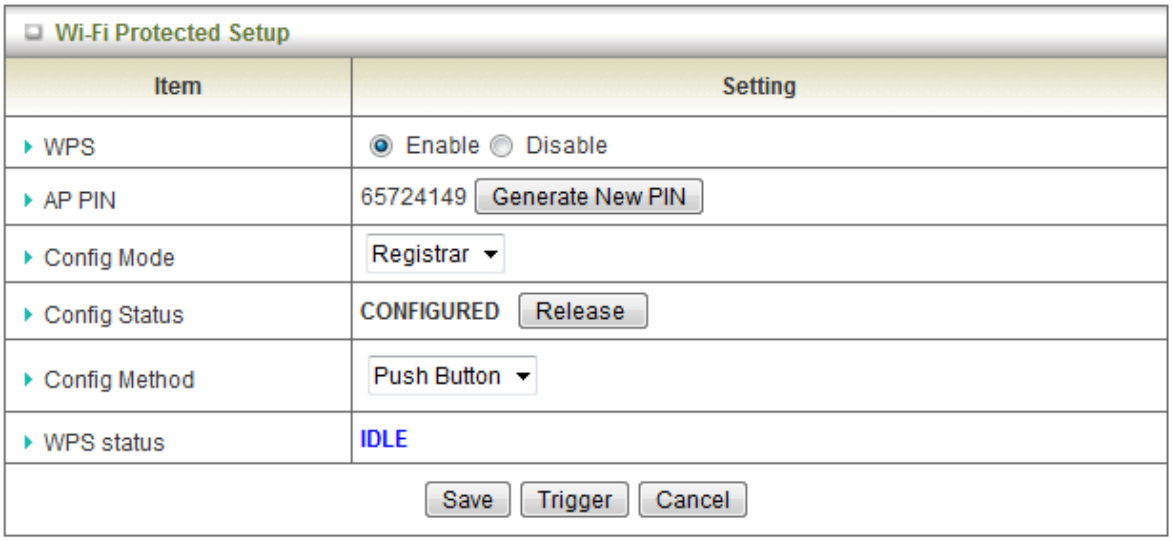
WDS (Wireless Distribution System) Setting

WDS operation as defined by the IEEE802.11 standard has been made available. Using WDS it is possible to wirelessly connect Access Points, and in doing so extend a wired infrastructure to locations where cabling is not possible or inefficient to implement.



WPS (Wi-Fi Protected Setup)

WPS is Wi-Fi Protected Setup which is similar to WCN-NET and offers safe and easy way in Wireless Connection.



Wireless Client List

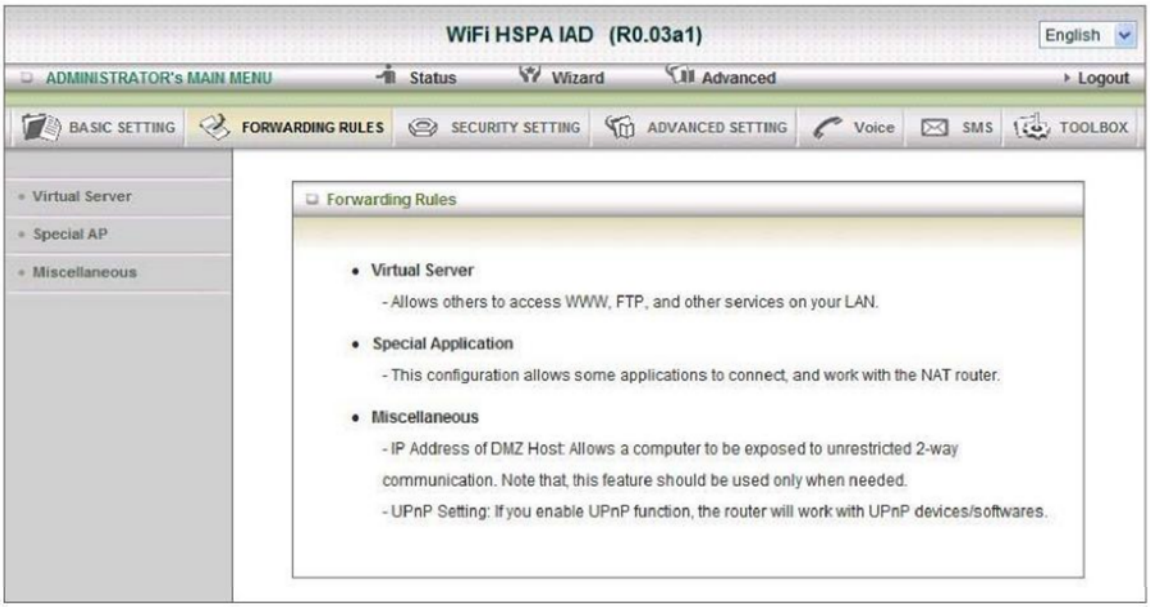
The list of wireless client is shows here.

3.2.1.4. Change Password

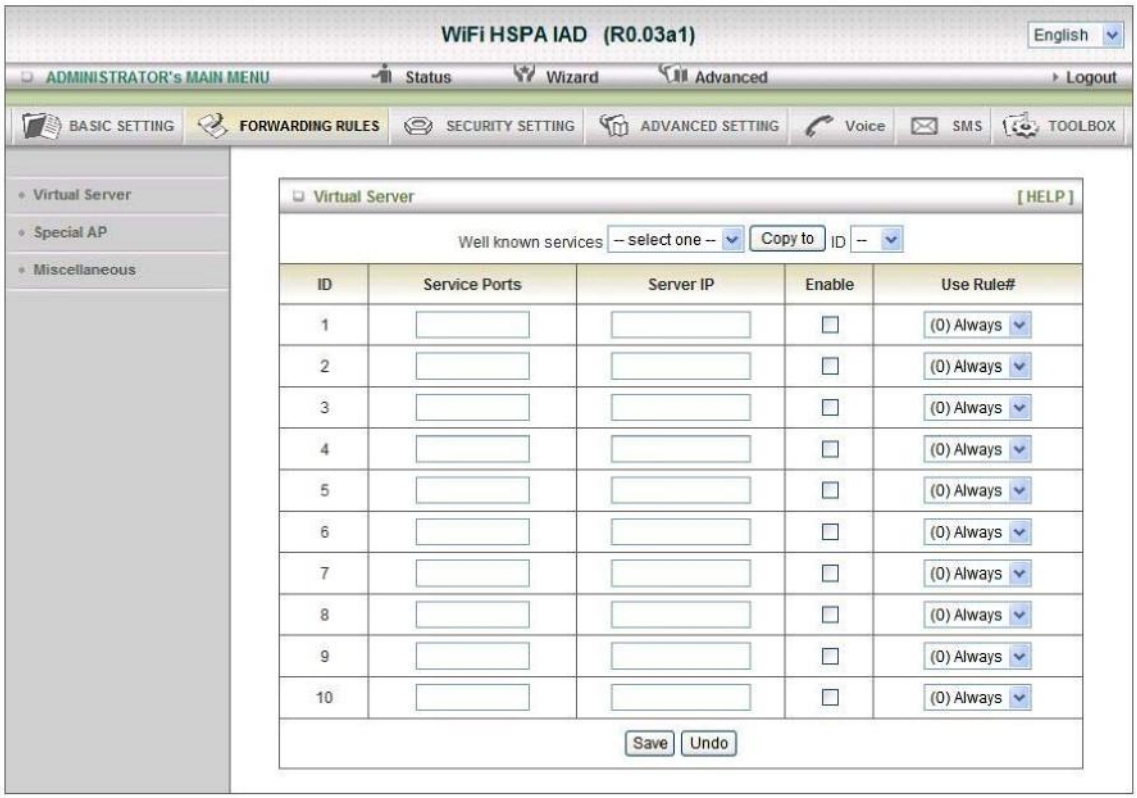
You can change Password here. We **strongly** recommend you to change the system password for security reason.

Click on “Save” to store your setting or “Undo” to give up

3.2.2. Forwarding Rules


WiFi HSPA IAD (R0.03a1)
English
ADMINISTRATOR's MAIN MENU
Status
Wizard
Advanced
Logout
BASIC SETTING
FORWARDING RULES
SECURITY SETTING
ADVANCED SETTING
Voice
SMS
TOOLBOX
Virtual Server
Special AP
Miscellaneous
Forwarding Rules
Virtual Server
- Allows others to access WWW, FTP, and other services on your LAN.
Special Application
- This configuration allows some applications to connect, and work with the NAT router.
Miscellaneous
- IP Address of DMZ Host: Allows a computer to be exposed to unrestricted 2-way communication. Note that this feature should be used only when needed.
- UPnP Setting: If you enable UPnP function, the router will work with UPnP devices/softwares.

3.2.2.1. Virtual Server



This product's NAT firewall filters out unrecognized packets to protect your Intranet, so all hosts behind this product are invisible to the outside world. If you wish, you can make some of them accessible by enabling the Virtual Server Mapping.

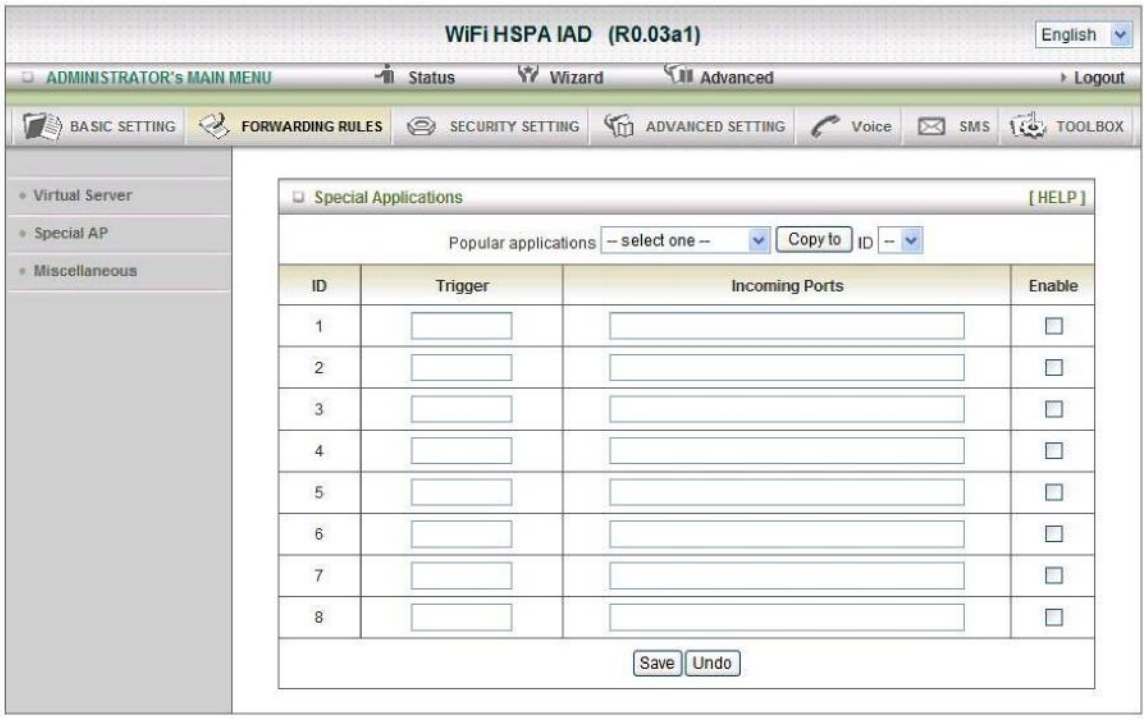
A virtual server is defined as a **Service Port**, and all requests to this port will be redirected to the computer specified by the **Server IP. Virtual Server** can work with **Scheduling Rules**, and give the user more flexibility on Access control. For Detail, please refer to **Scheduling Rule**.

For example, if you have an FTP server (port 21) at 192.168.1.1, a Web server (port 80) at 192.168.1.2, and a VPN server at 192.168.1.6, then you need to specify the following virtual server mapping table:

Service Port	Server IP	Enable
21	192.168.1.1	V
80	192.168.1.2	V
1723	192.168.1.6	V

Click on "Save" to store your setting or "Undo" to give up

3.2.2.2. Special AP



Some applications require multiple connections, like Internet games, Video conferencing, Internet telephony, etc. Because of the firewall function, these applications cannot work with a pure NAT router. **The Special Applications** feature allows some of these applications to work with this product. If the mechanism of Special Applications fails to make an application work, try setting your computer as the DMZ host instead.

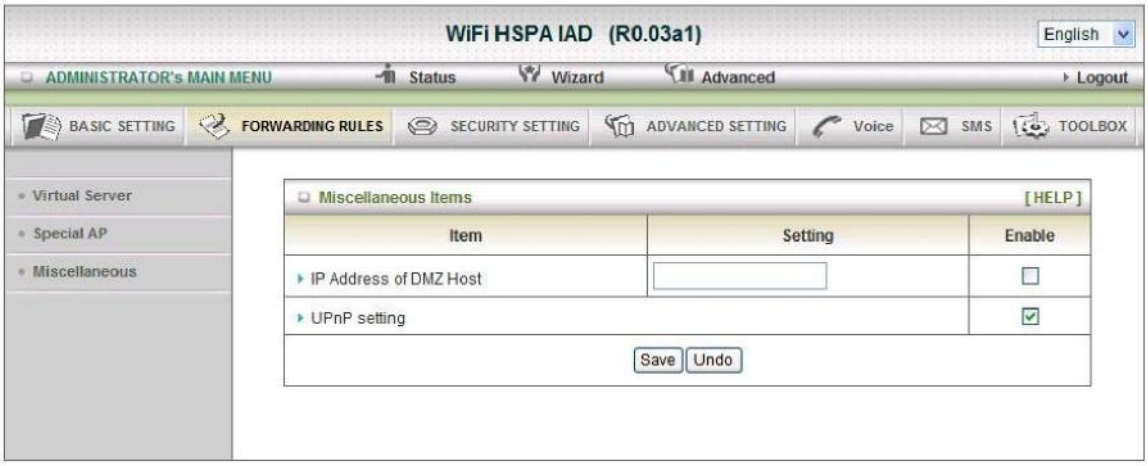
1. **Trigger:** the outbound port number issued by the application.
2. **Incoming Ports**: when the trigger packet is detected, the inbound packets sent to the specified port numbers are allowed to pass through the firewall.

This product provides some predefined settings.

Select your application and Click "**Copy to"** to add the predefined setting to your list.

Click on "Save" to store your setting or" Undo" to give up

3.2.2.3. Miscellaneous



1. **IP Address of DMZ Host**

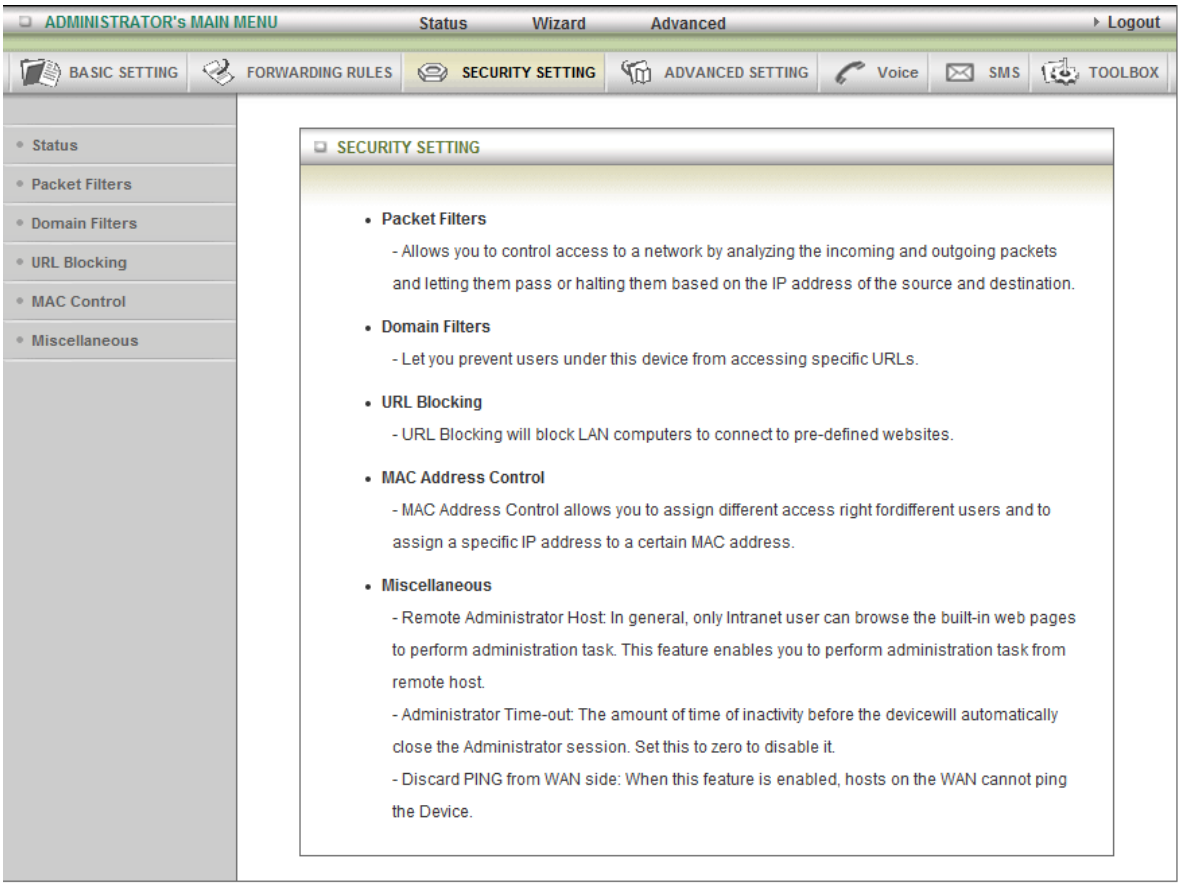
   DMZ (Demilitarized Zone) Host is a host without the protection of firewall. It allows a computer to be exposed to unrestricted 2-way communication for Internet games, Video conferencing, Internet telephony and other special applications.

2. **UPnP Setting**

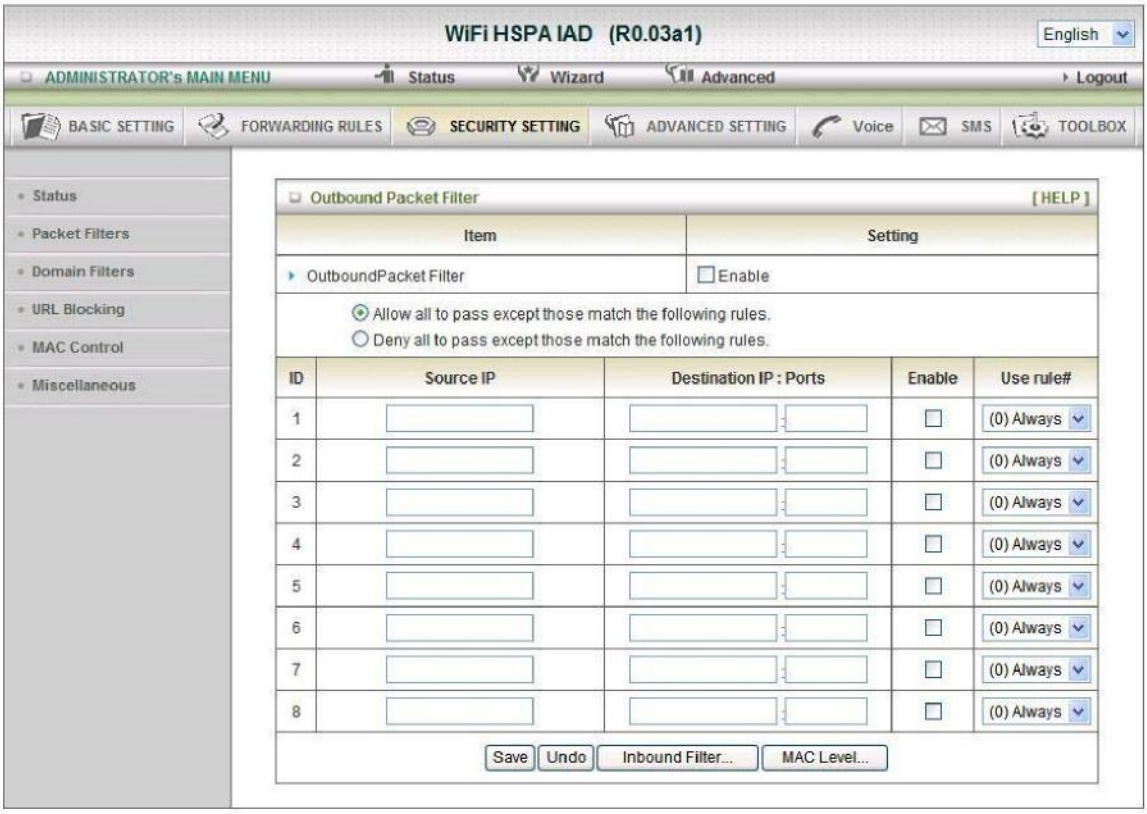
   The device also supports this function. If the OS supports this function enable it, like Windows XP. When the user gets IP from Device and will see icon as below:

Click on "Save" to store your setting or "Undo" to give up

3.2.3. Security Setting


ADMINISTRATOR's MAIN MENU
Status
Wizard
Advanced
Logout
BASIC SETTING
FORWARDING RULES
SECURITY SETTING
ADVANCED SETTING
Voice
SMS
TOOLBOX
Status
Packet Filters
Domain Filters
URL Blocking
MAC Control
Miscellaneous
SECURITY SETTING
Packet Filters
- Allows you to control access to a network by analyzing the incoming and outgoing packets and letting them pass or halting them based on the IP address of the source and destination.
Domain Filters
- Let you prevent users under this device from accessing specific URLs.
URL Blocking
- URL Blocking will block LAN computers to connect to pre-defined websites.
MAC Address Control
- MAC Address Control allows you to assign different access right fordifferent users and to assign a specific IP address to a certain MAC address.
Miscellaneous
- Remote Administrator Host: In general, only Intranet user can browse the built-in web pages to perform administration task. This feature enables you to perform administration task from remote host.
- Administrator Time-out: The amount of time of inactivity before the devicewill automatically close the Administrator session. Set this to zero to disable it.
- Discard PING from WAN side: When this feature is enabled, hosts on the WAN cannot ping the Device.

3.2.3.1. Packet Filters



Packet Filter includes both outbound filter and inbound filter. And they have same way to setting. Packet Filter enables you to control what packets are allowed to pass the router. Outbound filter applies on all outbound packets. However, inbound filter applies on packets that destined to Virtual Servers or DMZ host only. You can select one of the two filtering policies:

1. Allow all to pass except those match the specified rules
2. Deny all to pass except those match the specified rules

You can specify 8 rules for each direction: inbound or outbound. For each rule, you can define the following:

- Source IP address
- Source port
- Destination IP address
- Destination port
- Protocol: TCP or UDP or both.
- Use Rule#

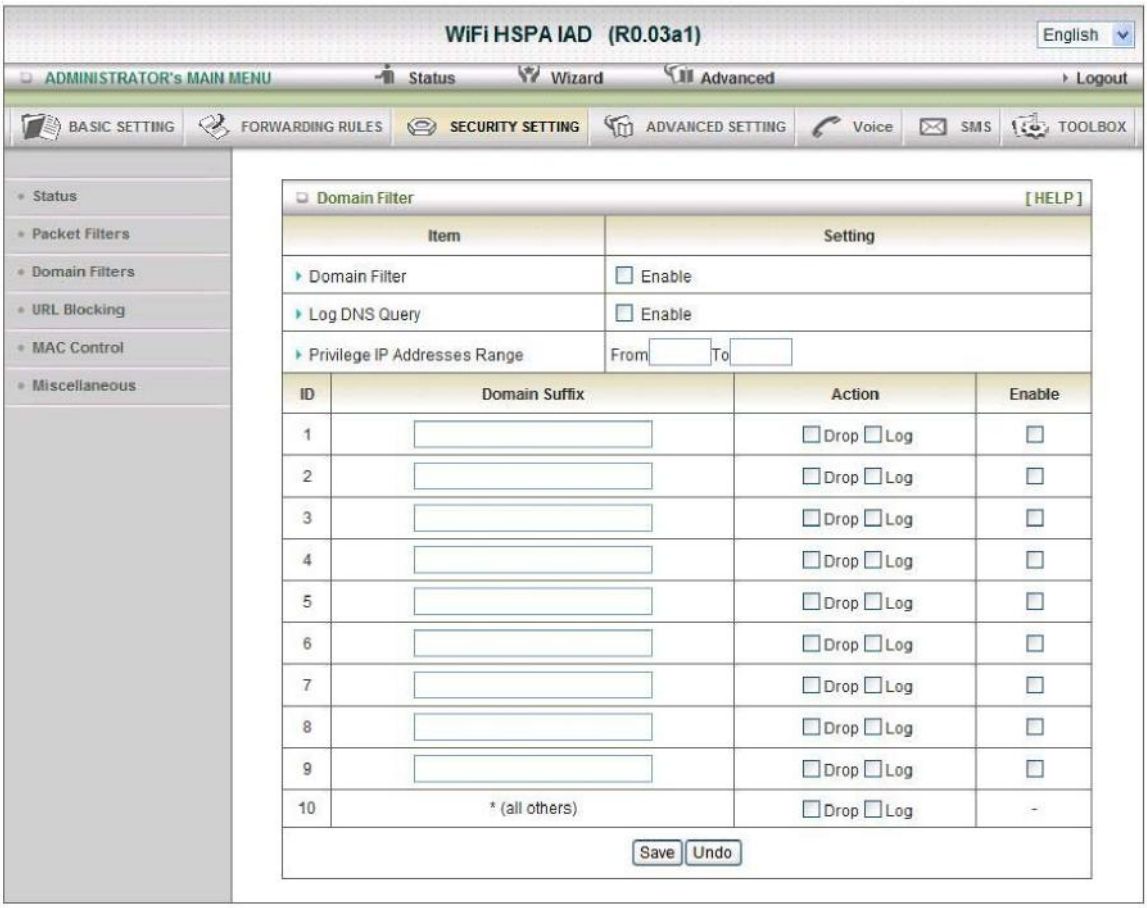
For source or destination IP address, you can define a single IP address (4.3.2.1) or a range of IP

addresses (4.3.2.1-4.3.2.254). An empty implies all IP addresses.
For source or destination port, you can define a single port (80) or a range of ports (1000-1999). Add prefix "T" or "U" to specify TCP or UDP protocol. For example, T80, U53, U2000-2999, No prefix indicates both TCP and UDP are defined. An empty implies all port addresses. Packet Filter can work with **Scheduling Rules,** and give user more flexibility on Access control. For Detail, please refer to **Scheduling Rule.**

Each rule can be enabled or disabled individually.

Click on “Save” to store your setting or “Undo” to give up

3.2.3.2. Domain Filters

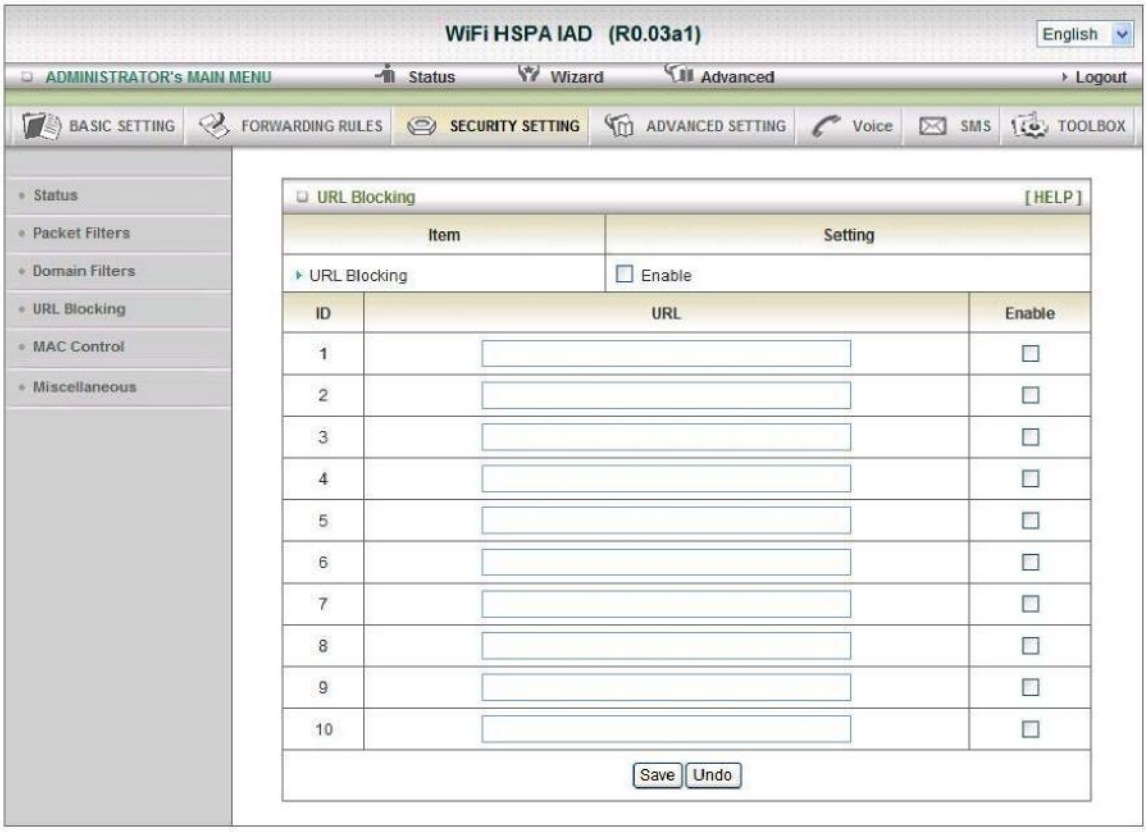


1. **Domain Filter** Let you prevent users under this device from accessing specific URLs.
2. **Domain Filter Enable** Check if you want to enable Domain Filter.
3. **Log DNS Query** Check if you want to log the action when someone accesses the specific URLs.
4. **Privilege IP Address Range** Setting a group of hosts and privilege these hosts to access network without restriction.
5. **Domain Suffix** A suffix of URL can be restricted, for example, ".com", "xxx.com".
6. **Action**
   When someone is accessing the URL met the domain-suffix, what kind of action you want. Check drop to block the access. Check “log” to log these access.
7. **Enable** Check to enable each rule.

Click on “Save” to store your setting or “Undo” to give up

3.2.3.3. URL Blocking

URL Blocking will block LAN computers to connect with pre-defined Websites. The major difference between “Domain filter” and “URL Blocking” is Domain filter require user to input suffix (like .com or .org, etc), while URL Blocking require user to input a keyword only. In other words, Domain filter can block specific website, while URL Blocking can block hundreds of websites by simply a **keyword**.



1. **URL Blocking Enable** Check if you want to enable URL Blocking.

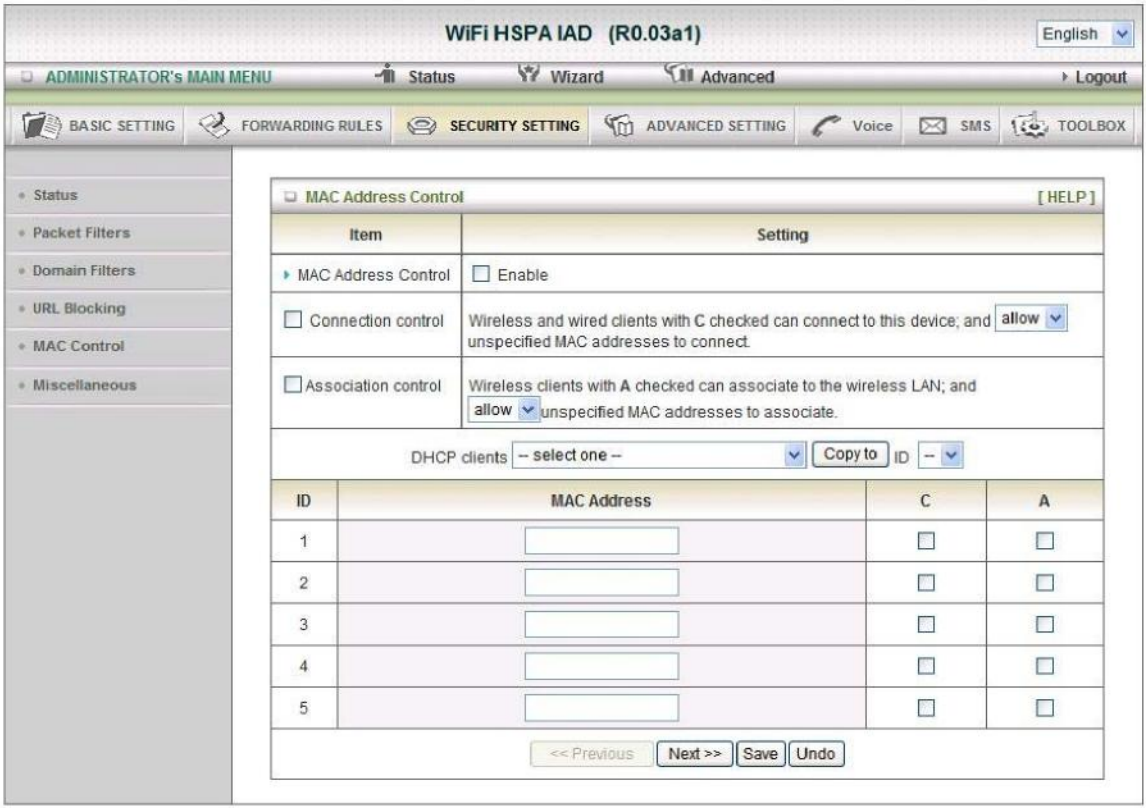
2. **URL**
If any part of the Website's URL matches the pre-defined word, the connection will be blocked.

For example, you can use pre-defined word "sex" to block all websites if their URLs contain pre-defined word "sex".

3. **Enable** Check to enable each rule.

Click on “Save” to store your setting or “Undo” to give up

3.2.3.4. MAC Control



MAC Address Control allows you to assign different access right for different users and to assign a specific IP address to a certain MAC address.

1. **MAC Address Control**

   Check “Enable” to enable the “MAC Address Control”. All of the settings in this page will take effect only when “Enable” is checked.

2. **Connection control**

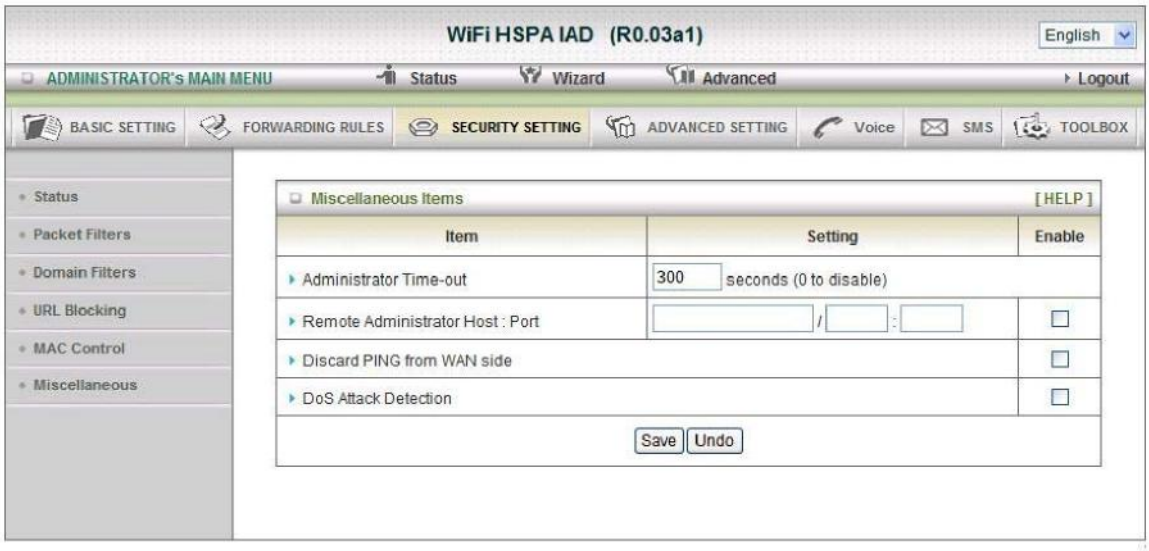
   Check "Connection control" to enable the controlling of which wired and wireless clients can connect with this device. If a client is denied to connect with this device, it means the client can't access to the Internet either. Choose "allow" or "deny" to allow or deny the clients, whose MAC addresses are not in the "Control table" (please see below), to connect with this device.

3. **Association control** Check "Association control" to enable the controlling of which wireless client can associate

to the wireless LAN. If a client is denied to associate to the wireless LAN, it means the client can't send or receive any data via this device. Choose "allow" or "deny" to allow or deny the clients, whose MAC addresses are not in the "Control table", to associate to the wireless LAN

Click “Save” to store your setting or “Undo” to give up

3.2.3.5. Miscellaneous



1. **Administrator Time-out** The time of no activity to logout automatically, you may set it to zero to disable this feature.

2. **Remote Administrator Host/Port**

   In general, only Intranet user can browse the built-in web pages to perform administration task. This feature enables you to perform administration task from remote host. If this feature is enabled, only the specified IP address can perform remote administration. If the specified IP address is 0.0.0.0, any host can connect with this product to perform administration task. You can use subnet mask bits "/nn" notation to specified a group of trusted IP addresses for example, "10.1.2.0/24".

   NOTE: When Remote Administration is enabled, the web server port will be shifted to 80. You can change web server port to other port, too.

3. **Discard PING from WAN side** When this feature is enabled, any host on the WAN cannot ping this product.

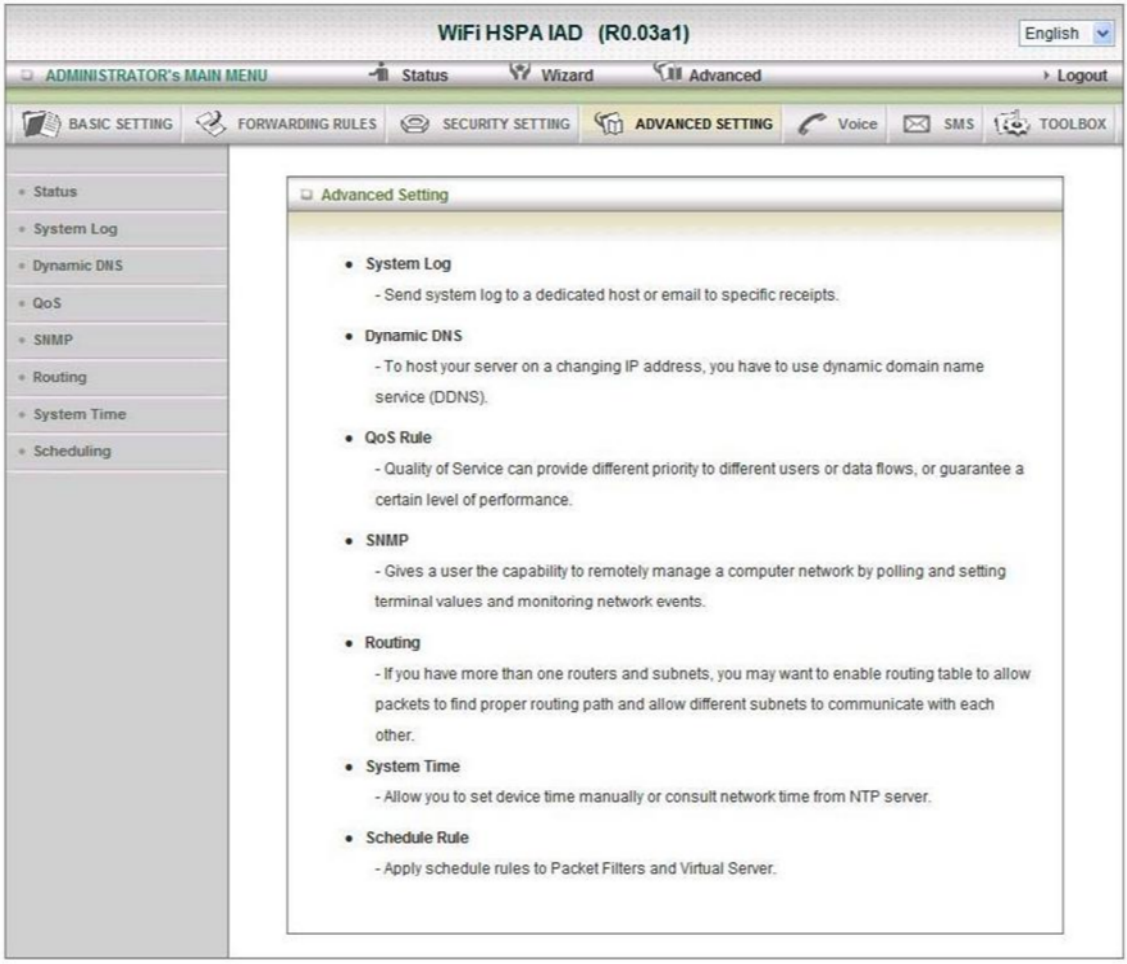
4. **DoS Attack Detection** When this feature is enabled, the router will detect and log the DoS attack comes from the

   Internet. Currently, the router can detect the following DoS attack: SYN Attack,

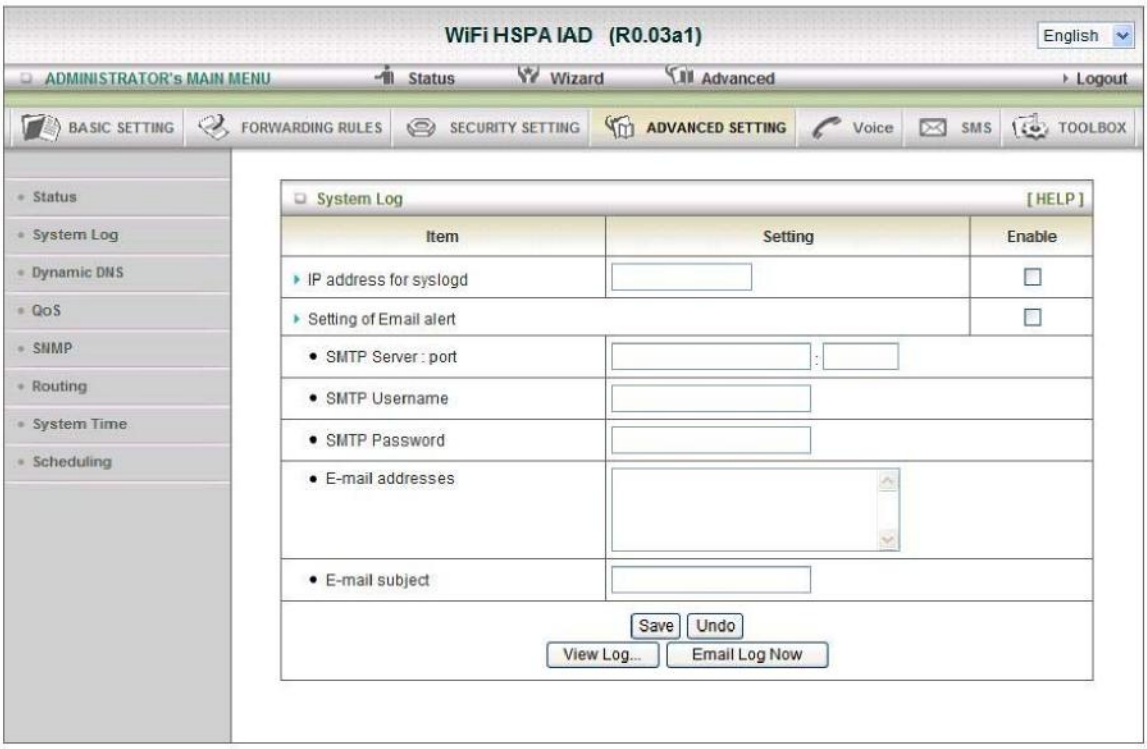
   WinNuke, Port Scan, Ping of Death, Land Attack etc.

Click on “Save” to store your setting or” Undo” to give up

3.2.4. Advanced Settings


WiFi HSPA IAD (R0.03a1)
English
ADMINISTRATOR's MAIN MENU
Status
Wizard
Advanced
Logout
BASIC SETTING
FORWARDING RULES
SECURITY SETTING
ADVANCED SETTING
Voice
SMS
TOOLBOX
Status
System Log
Dynamic DNS
QoS
SNMP
Routing
System Time
Scheduling
Advanced Setting
System Log
- Send system log to a dedicated host or email to specific receipts.
Dynamic DNS
- To host your server on a changing IP address, you have to use dynamic domain name service (DDNS).
QoS Rule
- Quality of Service can provide different priority to different users or data flows, or guarantee a certain level of performance.
SNMP
- Gives a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.
Routing
- If you have more than one routers and subnets, you may want to enable routing table to allow packets to find proper routing path and allow different subnets to communicate with each other.
System Time
- Allow you to set device time manually or consult network time from NTP server.
Schedule Rule
- Apply schedule rules to Packet Filters and Virtual Server.

3.2.4.1. System Log



This page support two methods to export system logs to specific destination by means of syslog (UDP) and SMTP(TCP). The items you have to setup including:

IP Address for Sys log

Host IP of destination where sys log will be sent to.
Check **Enable** to enable this function.

Setting of E-mail Alert

Check if you want to enable Email alert (send syslog via email).

SMTP Server IP and Port

Input the SMTP server IP and port, which are connected with ':'. If you do not specify port number, the default value is 25.

For example, "mail.your_url.com" or "192.168.1.100:26".

SMTP Username and Password

Input a user account and password for the SMTP server.

E-mail address

The recipients who will receive these logs, you can assign more than 1 recipient, using ';' or ',' to separate these email addresses.

E-mail Subject

The subject of email alert, this setting is optional.

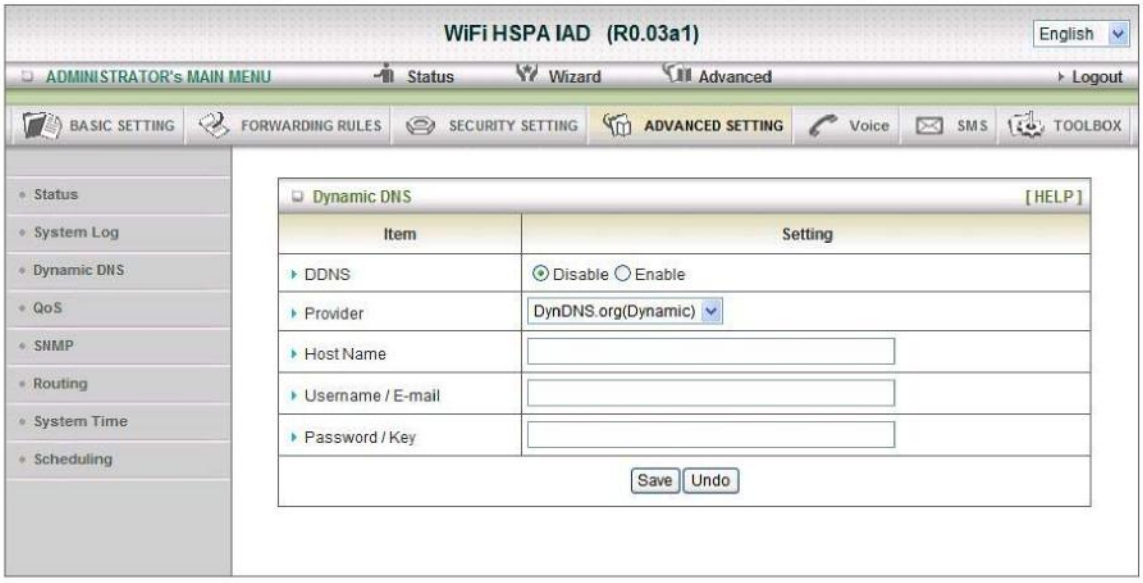
View Log...

Reference the section Toolbox/System Info

Click on “Save” to store your setting or “Undo” to give up

3.2.4.2. Dynamic DNS

To host your server on a changing IP address, you have to use dynamic domain name service (DDNS).



So that anyone wishing to reach your host only needs to know the name of it. Dynamic DNS will map the name of your host to your current IP address, which changes each time you connect your Internet service provider.

Before you enable **Dynamic DNS**, you need to register an account on one of these Dynamic DNS servers that we list in **provider** field.

To enable **Dynamic DNS** click the check box next to **Enable** in the **DDNS** field.

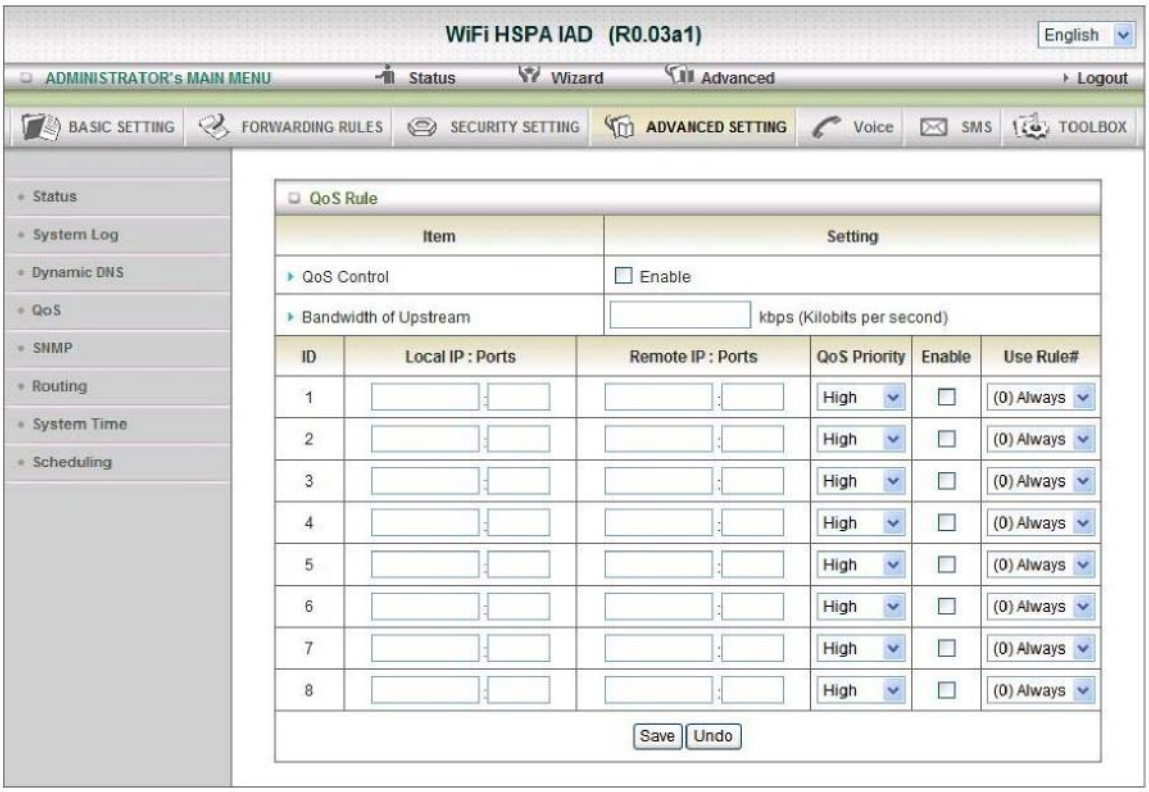
Next you can enter the appropriate information about your Dynamic DNS Server.
You have to define:

Provider
Host Name
Username/E-mail
Password/Key

You will get this information when you register an account on a Dynamic DNS server.

Click on “Save” to store your setting or “Undo” to give up

3.2.4.3. QOS



Provide different priority to different users or data flows, or guarantee a certain level of performance.

Enable

This Item enables QoS function or not.

Bandwidth of Upstream

Set the limitation of upstream speed.

Local: IP

Define the Local IP address of packets here.

Local: Ports

Define the Local port of the packets in this field.

Remote: IP

Define the Remote IP address of packets here.

Remote: Ports

Define the Remote port of the packets in this field.

QoS Priority

This defines the priority level of the current Policy Configuration. Packets associated with this policy will be serviced based upon the priority level set. For critical applications High or Normal levels are recommended. For non-critical applications select a Low level.

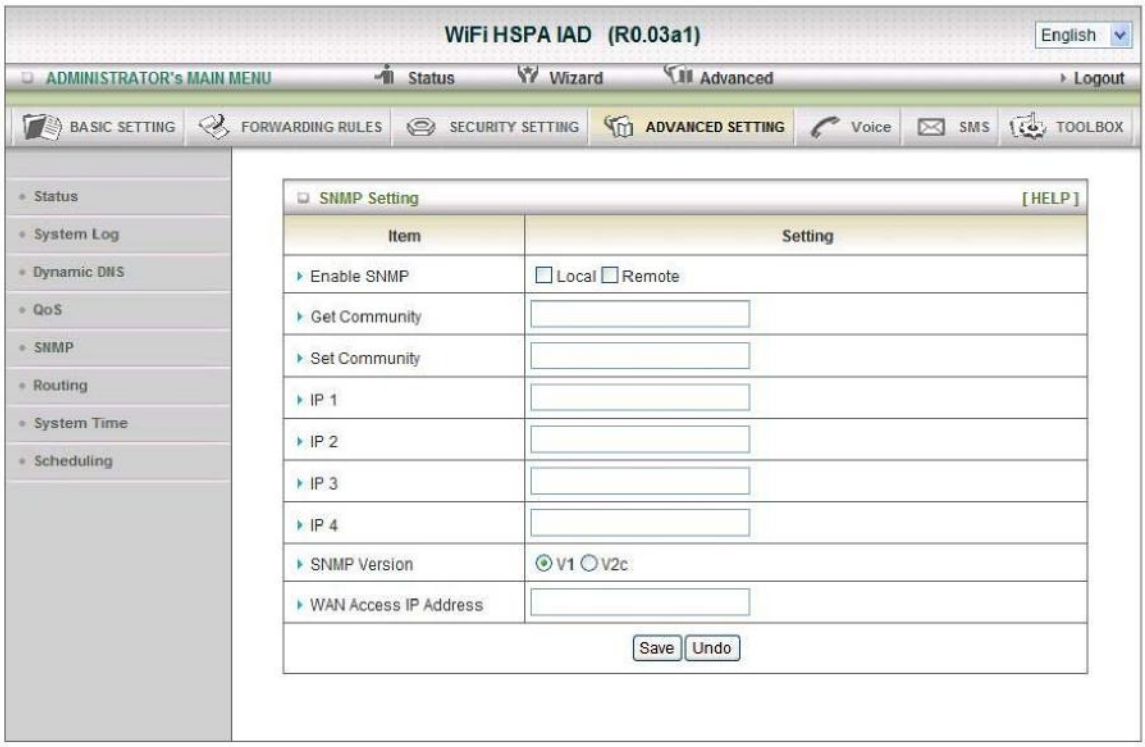
User Rule#

The QoS item can work with Scheduling Rule number#. Please reference the section Advanced

setting/schedule Rule.

Click on “Save” to store your setting or “Undo” to give up

3.2.4.4. SNMP



In brief, SNMP, the Simple Network Management Protocol, is a protocol designed to give a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.

Enable SNMP

You must check Local, Remote or both to enable SNMP function. If Local is checked, this device will response request from LAN. If Remote is checked, this device will response request from WAN.

Get Community

Setting the community of GetRequest your device will response.

Set Community

Setting the community of SetRequest your device will accept.

IP 1, IP 2, IP 3, IP 4

Input your SNMP Management PC’s IP here. User has to configure to where this device should send SNMP Trap message.

SNMP Version

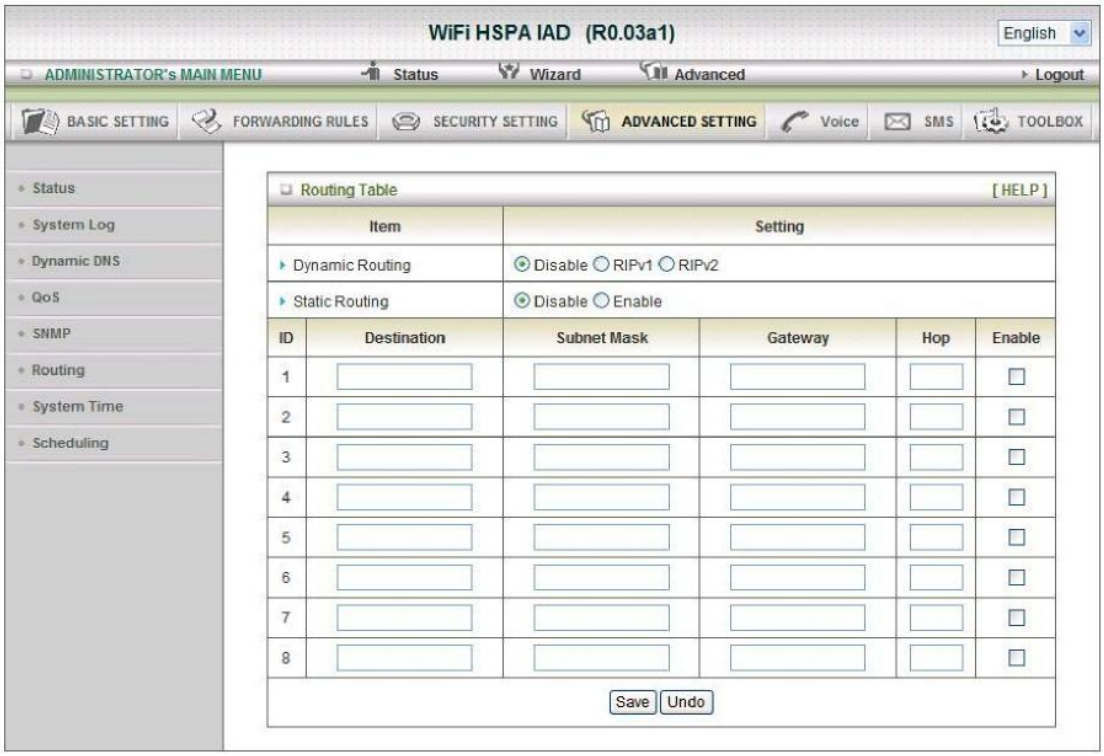
Please select proper SNMP Version that your SNMP Management software supports.

WAN Access IP Address

If the user wants to limit to specific the IP address to access, please input in the item. The default 0.0.0.0 and means every IP of Internet can get some information of device with SNMP protocol.

Click on “Save” to store your setting or “Undo” to give up.

3.2.4.5. Routing



Routing Tables

Allow you to determine which physical interface address to use for outgoing IP data grams. If you have more than one routers and subnets, you will need to enable routing table to allow packets to find proper routing path and allow different subnets to communicate with each other.

Routing Table settings are settings used to setup the functions of static and dynamic routing.

Dynamic Routing

Routing Information Protocol (RIP) will exchange information about destinations for computing routes throughout the network. Please select RIPv2 only if you have different subnet in your network. Otherwise, please select RIPv1 if you need this protocol.

Static Routing

For static routing, you can specify up to 8 routing rules. You can enter the destination IP address, subnet mask, gateway, hop for each routing rule, and then enable or disable the rule by checking

or un-checking the Enable checkbox.

Click on “Save” to store your setting or “Undo” to give up.

3.2.4.6. System Time

Time Zone

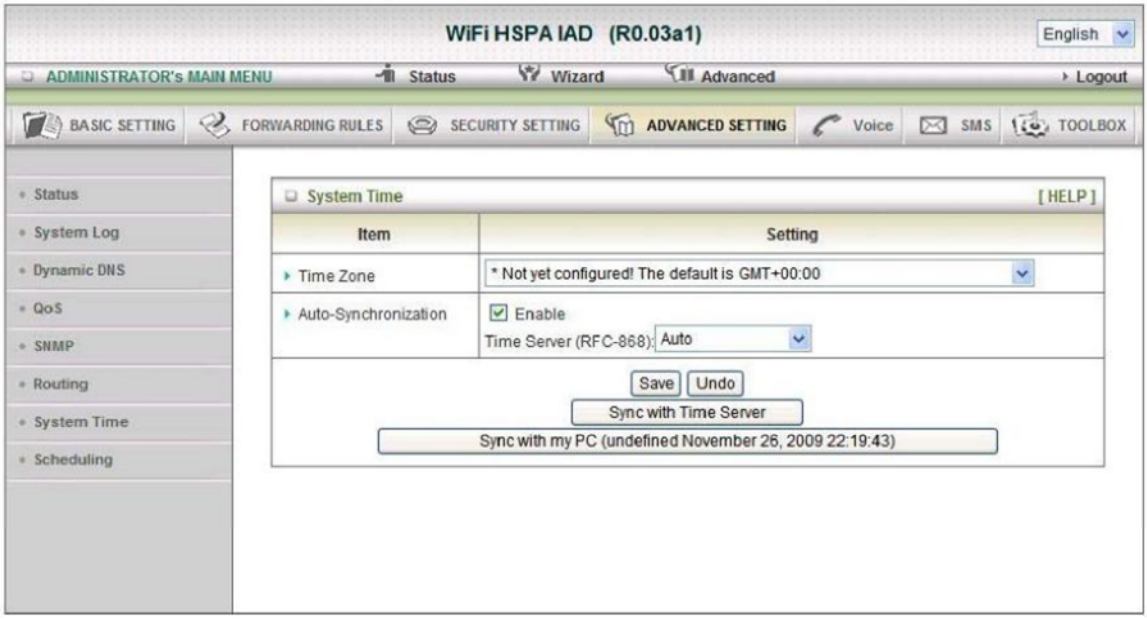
Select a time zone where this device locates. **Auto-Synchronization**

Select the “Enable” item to enable this function.

Time Server

Select a NTP time server to consult UTC time

Sync with Time Server

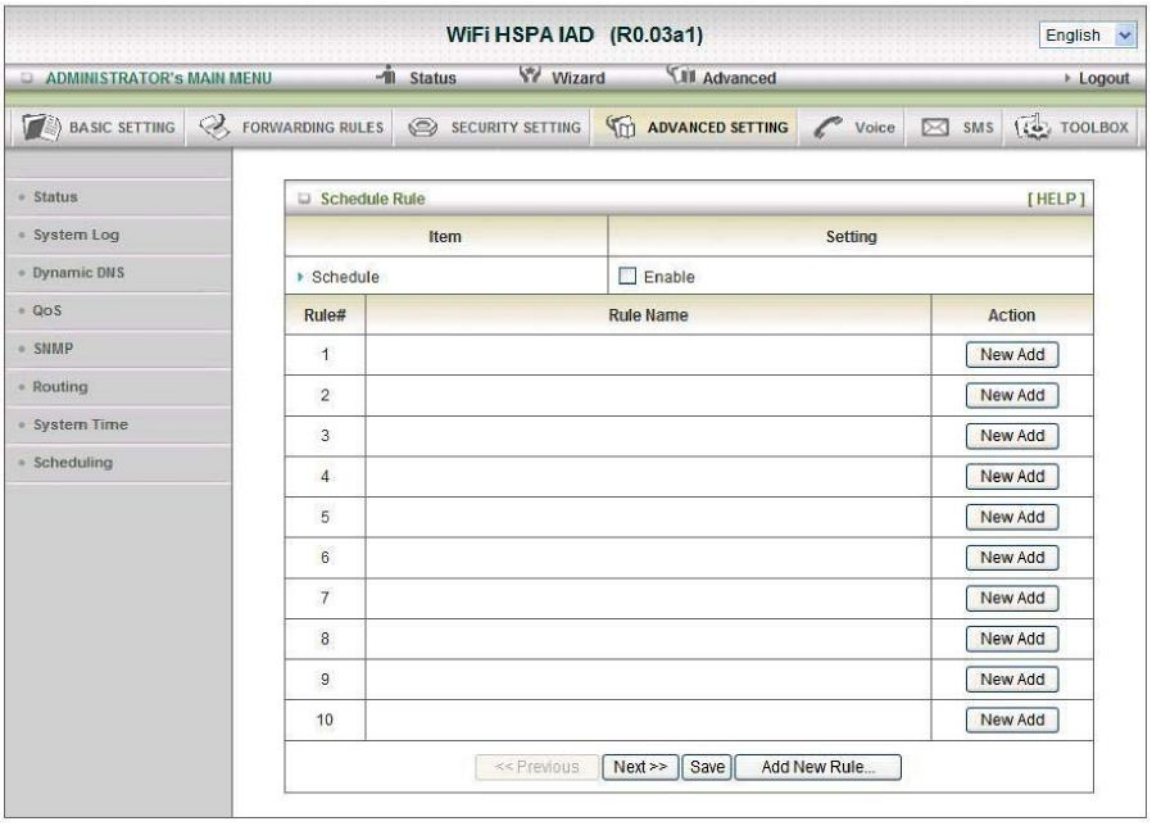


Select if you want to set Date and Time by NTP Protocol. **Sync with my PC**

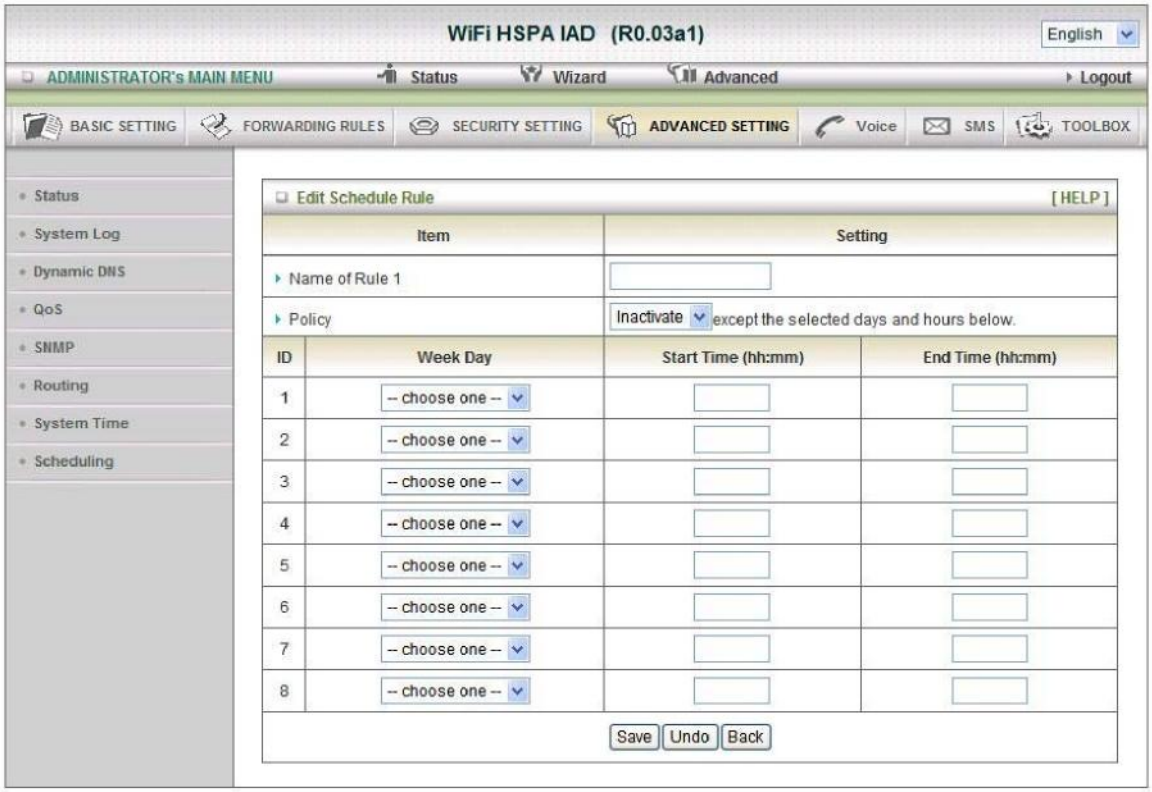
Select if you want to set Date and Time using PC’s Date and Time

Click on “Save” to store your setting or “Undo” to give up.

3.2.4.7.Scheduling

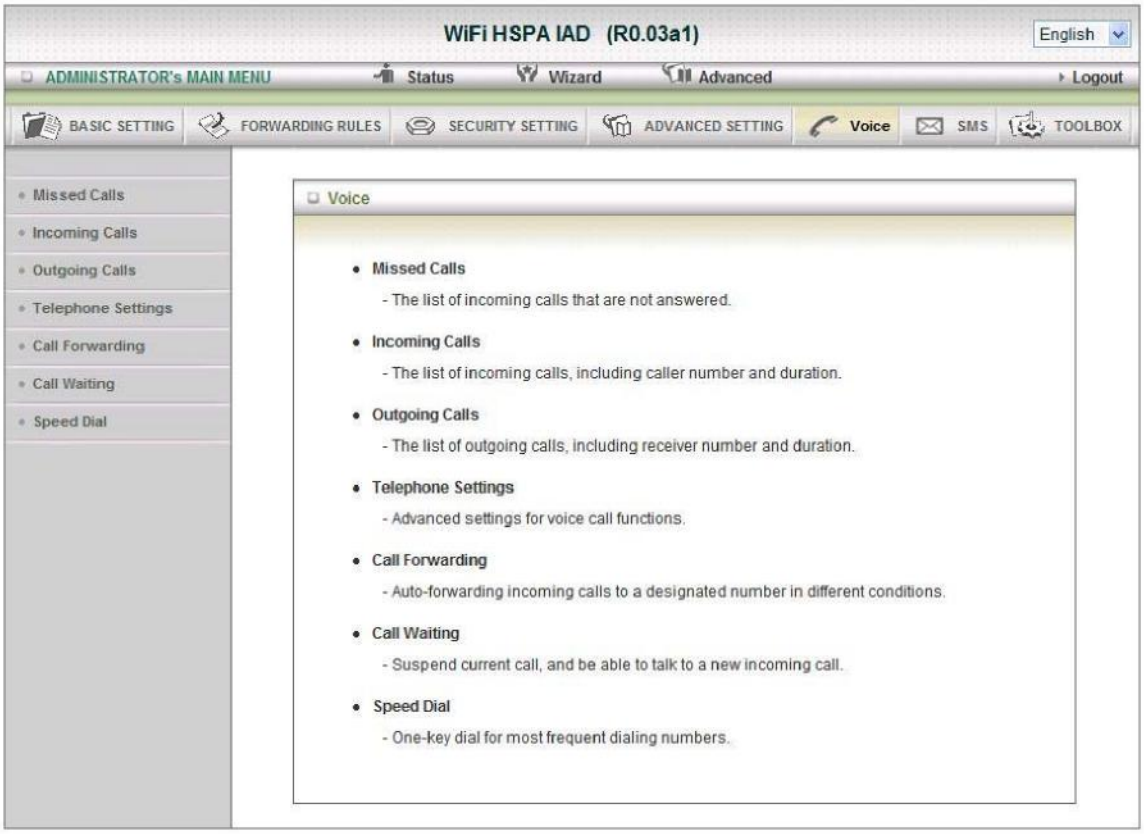


You can set the schedule time to decide which service will be turned on or off.
Select the “Enable” item. Press “Add New Rule” You can write a rule name and set which day and what time to schedule from “Start Time” to “End Time”. The following example configure “ftp time” as everyday 14:10 to 16:20



Click on “Save” to store your setting.

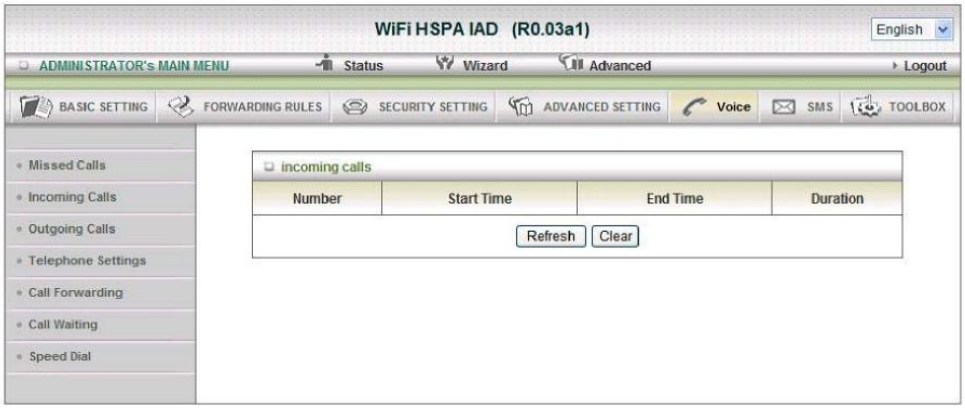
3.2.5. Voice



3.2.5.1. Missed Calls

The page is for incoming calls which are not answered, including receiver number and duration.

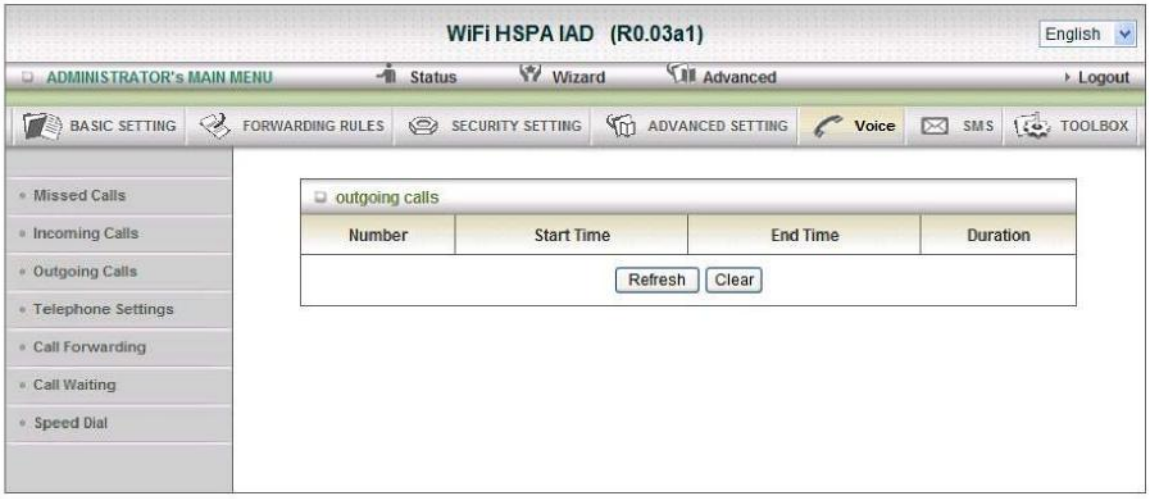
3.2.5.2. Incoming Calls



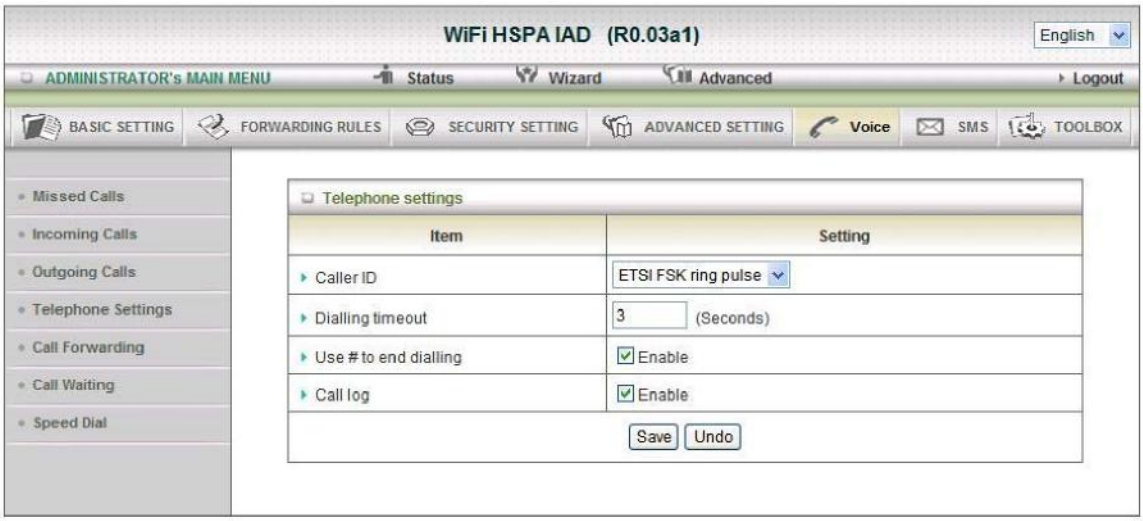
The page is for incoming calls which are answer, including receiver number and duration.

3.2.5.3. Outgoing Calls

The page is for outgoing calls, including receiver number and duration.



3.2.5.4. Telephone settings



Advanced settings for voice call functions.

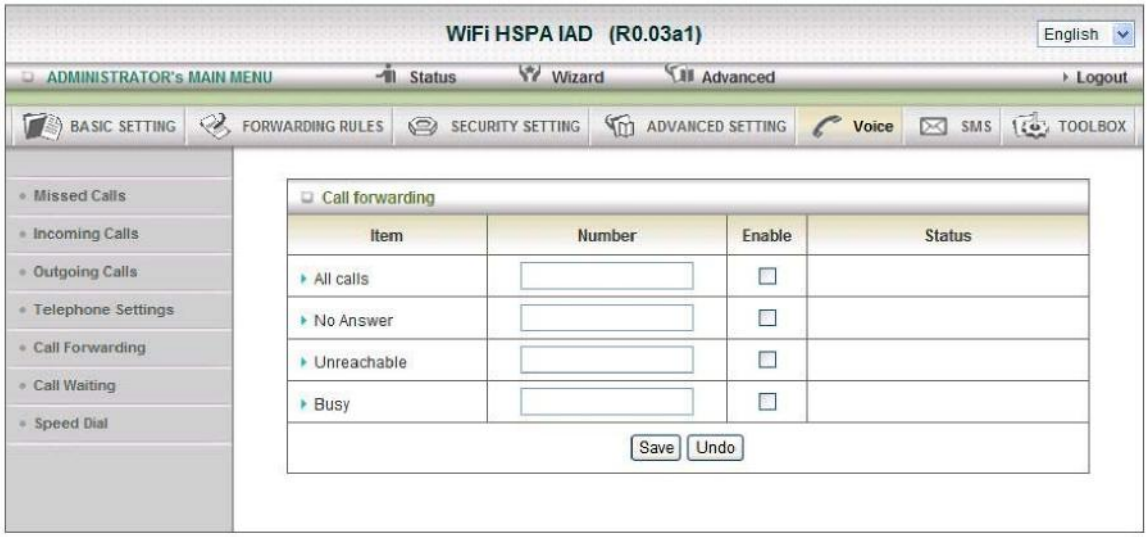
Caller ID: Calling number identification, two methods: FSK, DTMF.

Dialing timeout: the default value is 3 seconds.

Use # to end dialing: Enable or Disable the “Use # to end dialing”.

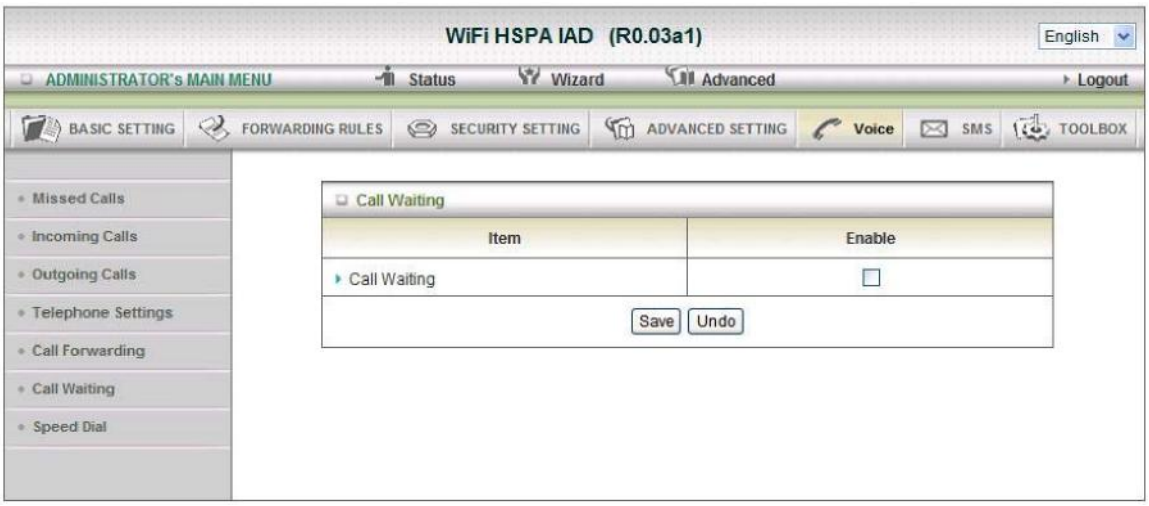
Call log: Enable or Disable the logs of Missed Call / Incoming Calls / Outgoing Calls

Call Forwarding



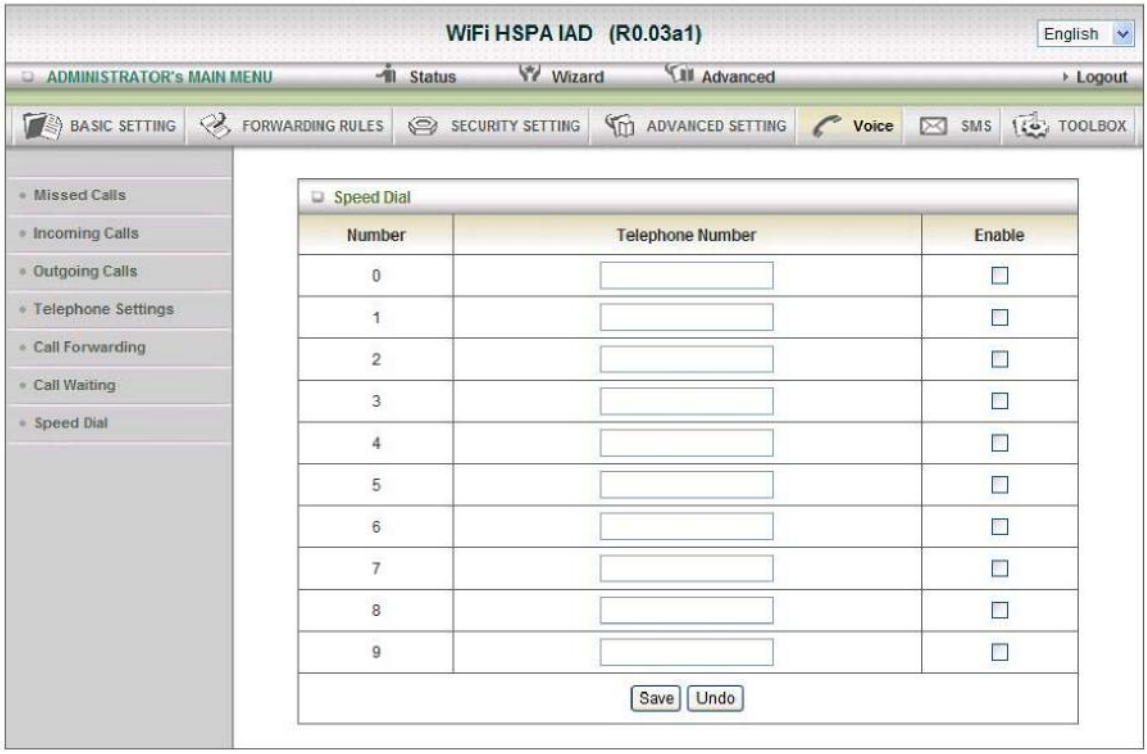
Auto-forwarding incoming calls to a designated number in different conditions: All calls / No Answer / Unreachable / Busy。

3.2.5.5. Call Waiting



Suspend current call, and be able to talk to a new incoming call.

3.2.5.6. Speed Dial

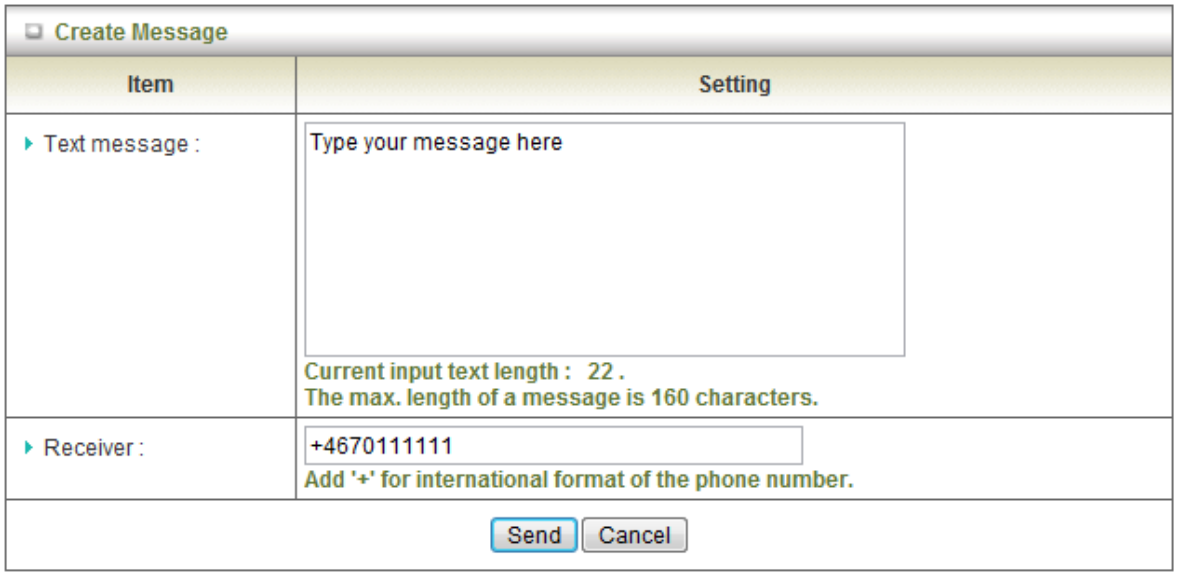


This page is for One-key dial for most frequent dialing numbers.

3.2.6. SMS

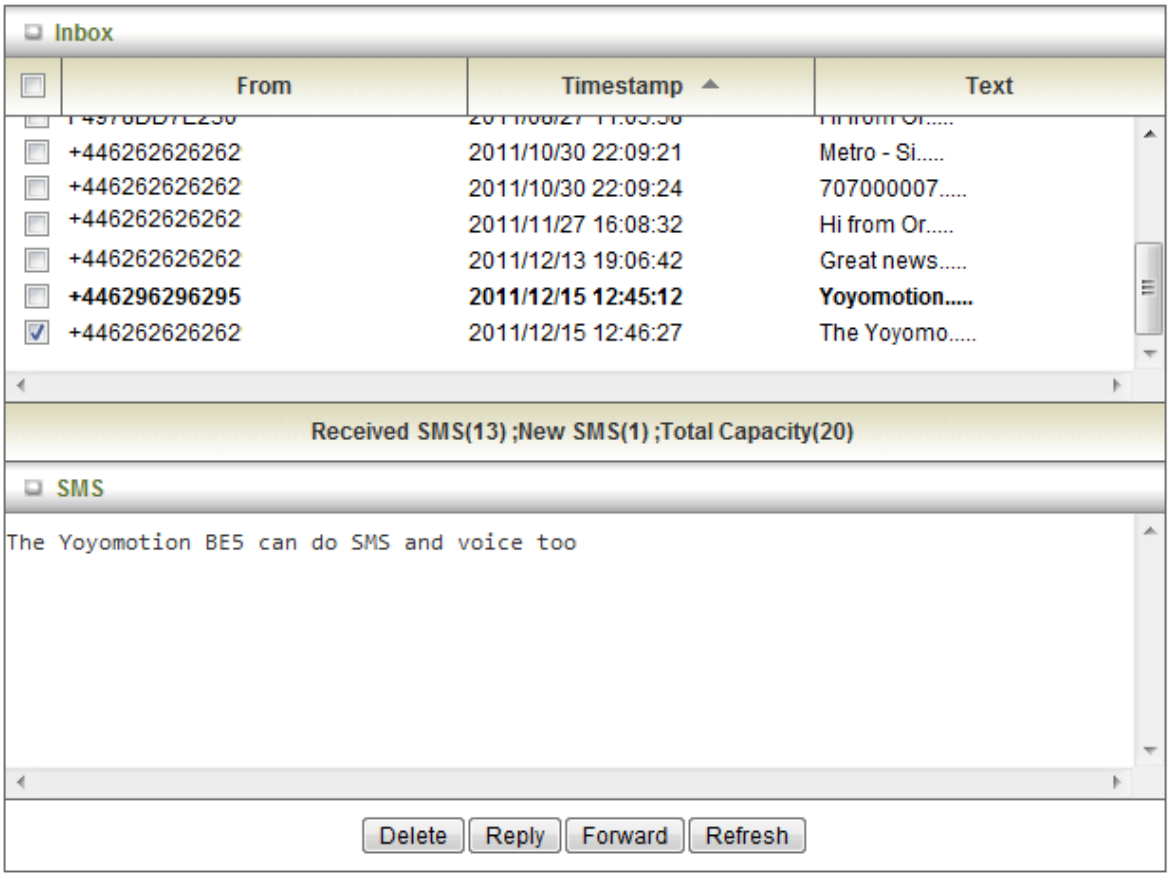
Select **Advanced** then **SMS** to work with SMS messages.

3.2.6.1. Create Message



You can create a new SMS message on this page. After finishing content of message, and enterting the phone number of recipient(s), press the **Send** button to send the message out. You can see “Send OK” if the new message has been sent successfully.

3.2.6.2. Inbox

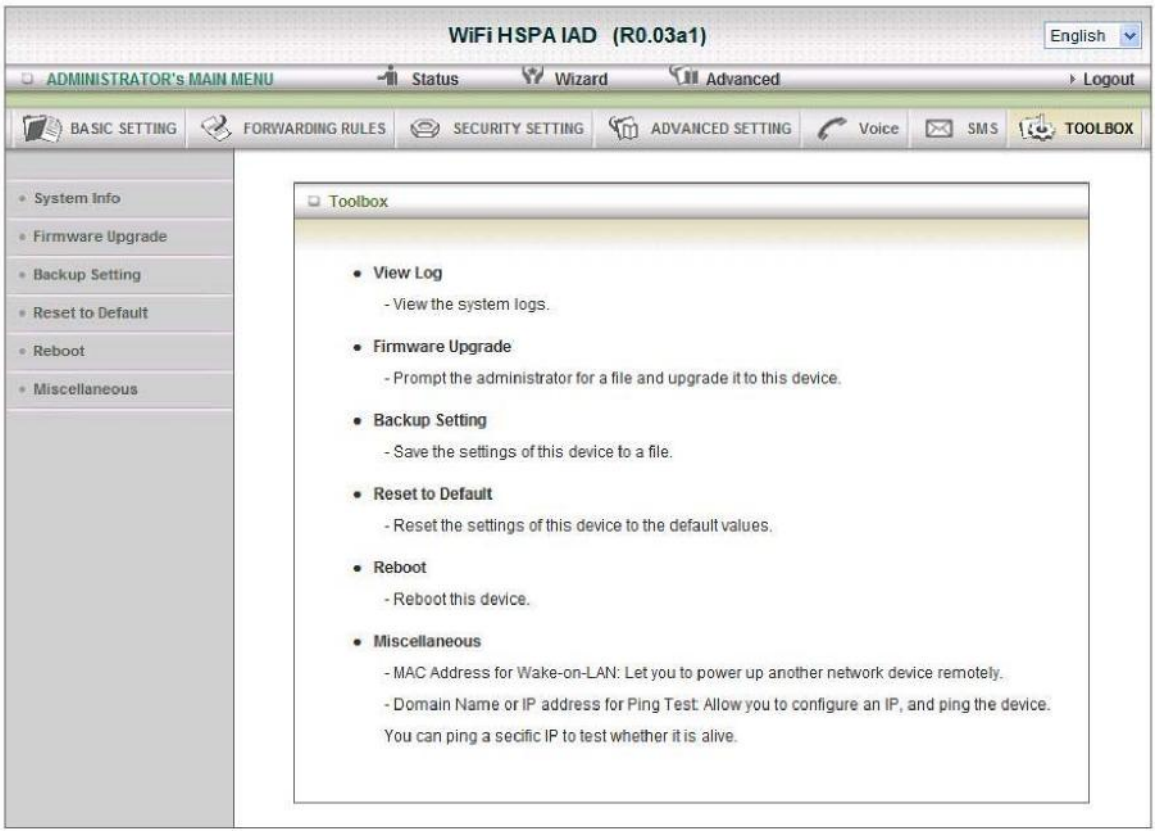


You can read, delete, reply, and forward messages. Just click on one in the Inbox, then you can view the whole content of it in the SMS window below.

Refresh:
You can press “Refresh” button to check for new messages.

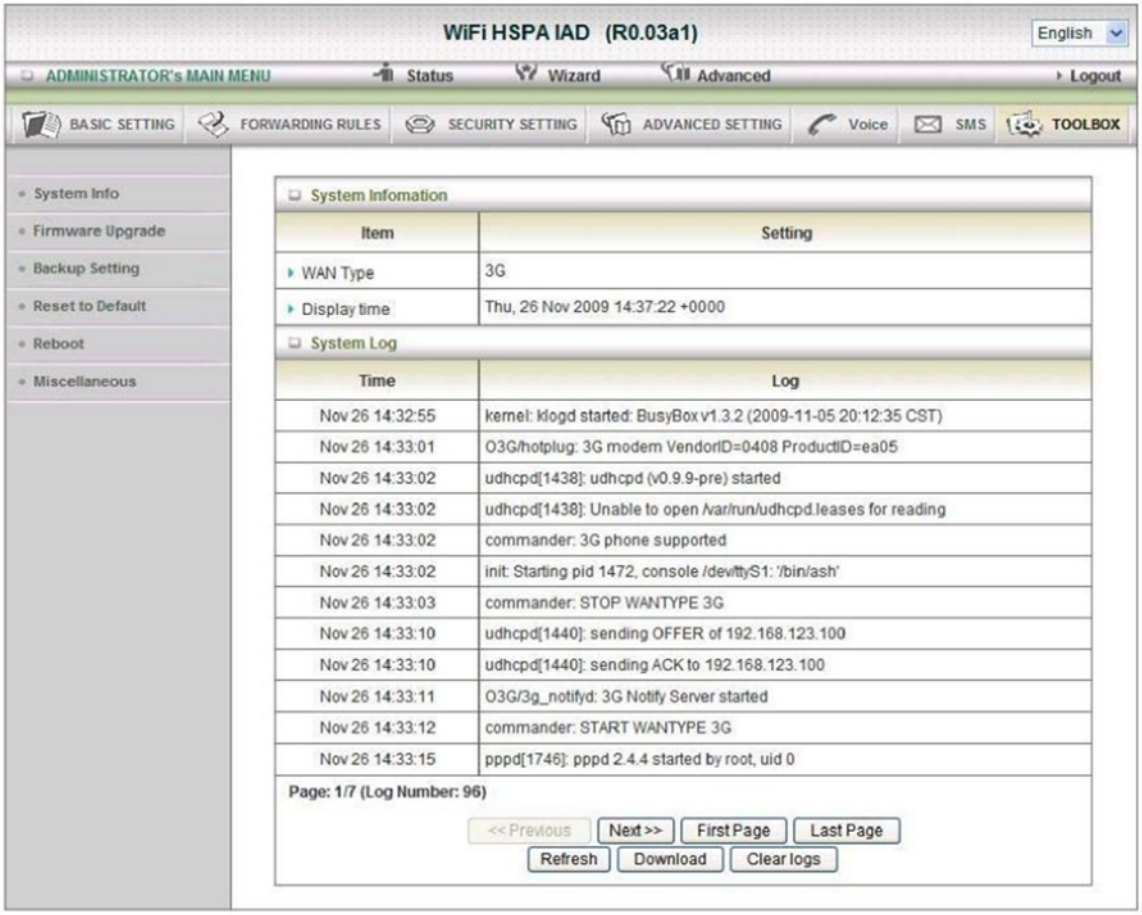
Delete, Reply, Forward Messages:
After reading message, you can check the checkbox on the left of each message to delete, reply, or forward this message.

3.2.7. Tool Box

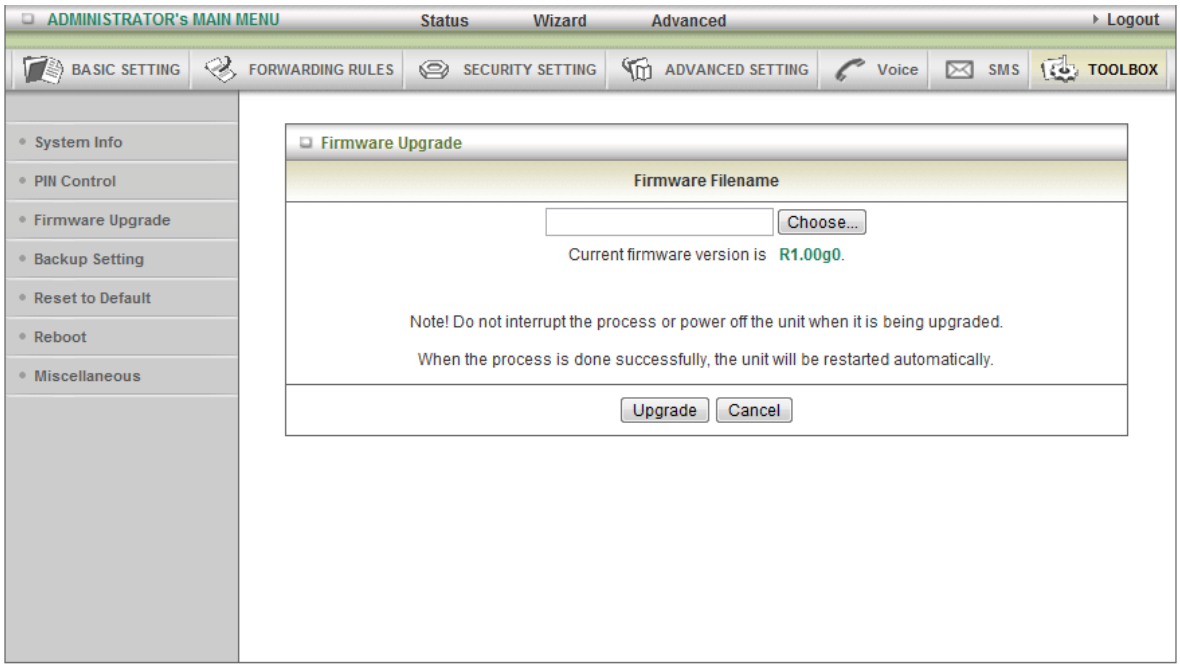

WiFi HSPA IAD (R0.03a1)
English
ADMINISTRATOR's MAIN MENU
Status
Wizard
Advanced
Logout
BASIC SETTING
FORWARDING RULES
SECURITY SETTING
ADVANCED SETTING
Voice
SMS
TOOLBOX
System Info
Firmware Upgrade
Backup Setting
Reset to Default
Reboot
Miscellaneous
Toolbox
View Log
- View the system logs.
Firmware Upgrade
- Prompt the administrator for a file and upgrade it to this device.
Backup Setting
- Save the settings of this device to a file.
Reset to Default
- Reset the settings of this device to the default values.
Reboot
- Reboot this device.
Miscellaneous
- MAC Address for Wake-on-LAN: Let you to power up another network device remotely.
- Domain Name or IP address for Ping Test: Allow you to configure an IP, and ping the device.
You can ping a secific IP to test whether it is alive.

3.2.7.1. System Info

You can view the System Information and System log, and download/clear the System log, in this page.



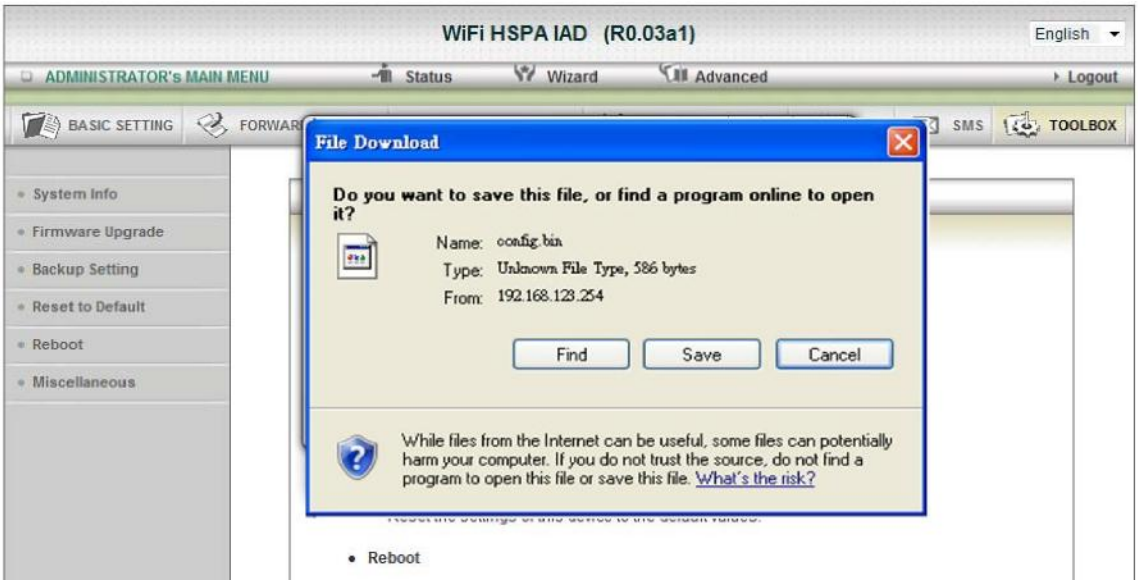
3.2.7.2. Firmware Upgrade



You can upgrade firmware by clicking “Upgrade”

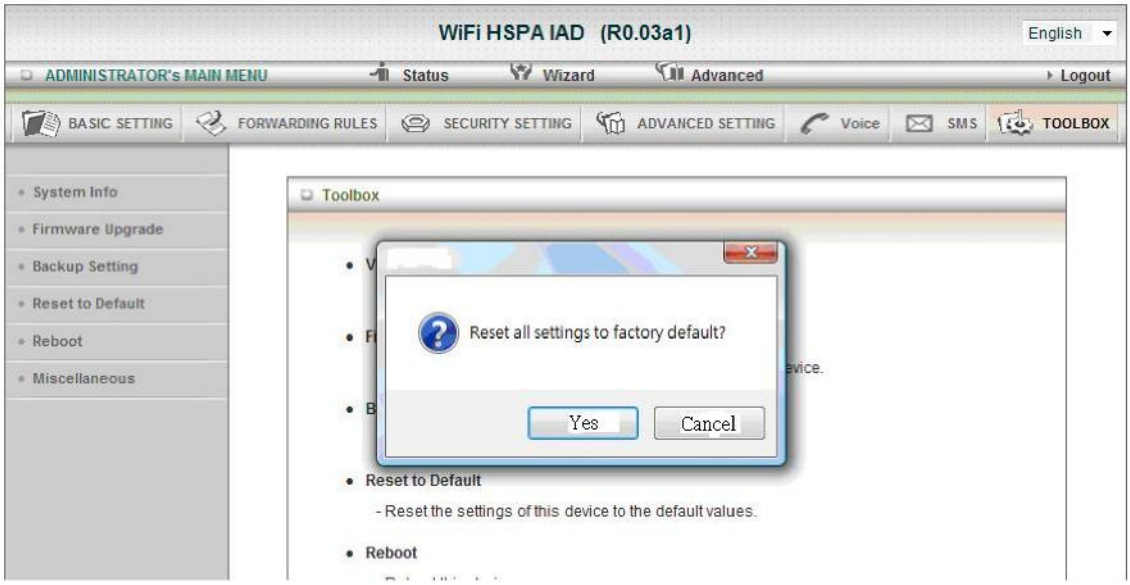
button.

3.2.7.3. Backup Setting



You can backup your settings by clicking the “**Backup Setting”** button and save it as a bin file. Once you want to restore these settings, please click Firmware Upgrade button and use the bin file you saved.

3.2.7.4. Reset to Default

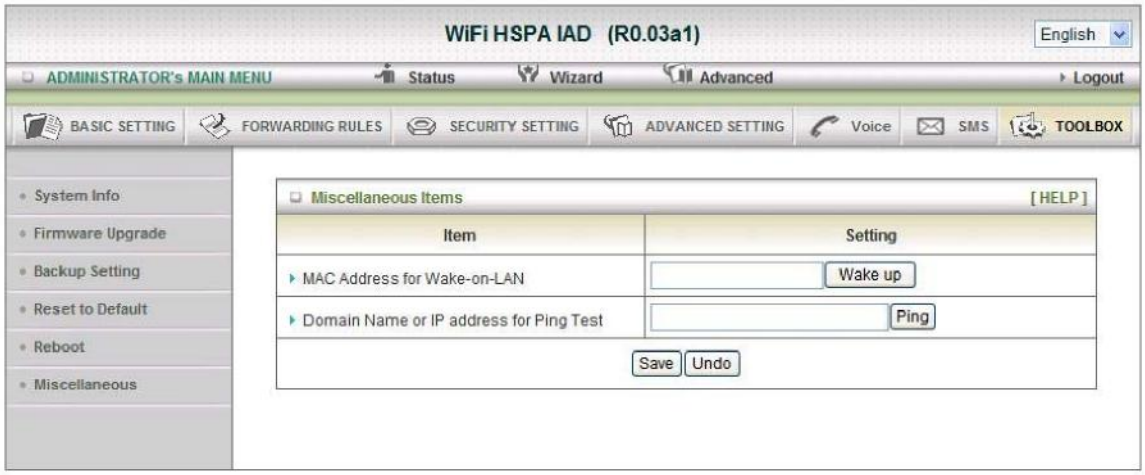


You can also reset this product to factory default by clicking the **Reset to default** button.

3.2.7.5. Reboot

You can also reboot this it by clicking the **Reboot** button.

3.2.7.6. Miscellaneous



Domain Name or IP address for Ping Test

Allow you to configure an IP, and ping the device. You can ping a specific IP to test whether it is alive.

4. Using the Telephone Feature

4.1. Overview

YOYORouter BE5 supports voice calls using a connected telephone. The calls are made using the mobile network.

Telephone features include:

- Use any standard analog Touch-Tone (DTMF) telephone connected to the RJ11 phone jack
- Outgoing calls by dialing or using any number storage features on the connected phone
- 10 outgoing call speed dials (shortcuts) stored in the BE5
- Incoming calls to the SIM Card voice number (MSISDN) ring on the connected phone
- Calling Line Identification (CLI) supported for compatible telephones.
- Call log maintained in the BE5 (Incoming, Outgoing, Missed)
- Call forwarding (as supported by the mobile operator)
- Call Waiting (as supported by the mobile operator)

To use the Telephone features:

- An analog telephone must be connected to the RJ11 telephone jack on the BE5
- A SIM Card must be plugged in
- The SIM card must support voice services
- The BE5 must have mobile service (2G or 3G)

Note: When the mobile service is 2G, the internet connection is suspended for the duration of each voice call. In other words, the 2G networks can support either voice or data but not both at the same time. Voice calls take precedence.

Note: Call logs and settings are available in the Advanced Settings of the Router. An Internet connection is necessary to synchronize with an Internet time server.

4.2. Using the Telephone

4.2.1. To make a call

1. Lift the receiver or press the make call button. (Consult the instructions for your connected telephone if necessary)
2. If voice service is available, the BE5 presents a dialing tone.
3. Dial the number or, if your connected phone has quick-dial buttons or an address book, use these features.
   Note: If you are dialing using the keypad, do not pause for more than three seconds in between digits. The BE5 interprets a three second pause as the end of the number. This pause time can be adjusted in the settings. You can also press the # key at the end of the number to tell the BE5 that the number is complete and can be dialed immediately.
4. The call is dialed over the mobile network
5. To end the call, replace the receiver or press the call end button, as necessary on your connected phone.

Note: Analog phones have no “+” key for international dialing. You will need to dial the appropriate numeric prefix for international, for example 00 in most of Europe or 011 in the USA and Canada.

If short codes have been configured in the settings, simply dial 0 (or 0#) to 9 (or 9#) to dial the

pre-selected short code.

4.2.2. To receive a call

1. The incoming call rings on the connected telephone.
2. If the connected telephone supports a CLI display that is compatible with BE5 and the calling number is available, it is displayed on the connected telephone.
3. Lift the receiver or press the answer button, according to the operation of the connected telephone.
4. When the call is over, replace the receiver or press the call end button, according to the operation of the connected telephone.

4.2.3. Admin Features

Settings for Telephony include Call Forwarding, Call Log etc are documented in the Reference > Voice section.

The Voice Admin features can be accessed by the administrator. They can also be accessed by typing password *YOYOguest* as the admin password. In this case only status, telephony and SMS features are presented.

5. Troubleshooting

This Chapter provides solutions to problems for the installation and operation of the YOYORouter. You can refer to the following if you are having problems.

5.1. Basic Problems

How to reset YOYORouter to factory state

Your YOYORouter can be reset to its factory state. This is useful if you have changed and forgotten the W-Fi network name (SSID) or Wi-Fi password.

To reset YOYORouter:

1. Switch on YOYORouter in Modem mode
2. Locate the Reset switch on the rear of YOYORouter B1.
3. Use a pencil or other tool, insert it in the Reset hole and gently press the Reset switch for at least 8 seconds.
4. YOYORouter restarts.

After Reset, YOYORouter will make its default configuration, which is suitable for most users. If necessary, re-configure your YOYORouter to your own needs.

The Wi-Fi network will have been changed to a network name (SSID) like **YOYORouter-12-34** where the numbers are particular to your example and printed on the label on the device itself and the carton in which it was supplied. The password is also printed on the label.

5.2. Wi-Fi Problems

I cannot find the Wi-Fi network

By default, YOYORouter's Wi-Fi network name (SSID) is like **YOYORouter-12-34** where the numbers are particular to your example and printed on the label on the device itself and the carton in which it was supplied.

- Try moving closer to YOYORouter
- On the device you are trying to connect, request it to re-scan for networks and see if YOYORouter-xx-xx appears.

If you have configured your YOYORouter to hide the SSID, it will not appear in the network list on any device you try to connect.

- You must select manual configuration and enter the network name and password.
- Or you must change the setting Advanced > Wireless > SSID Broadcast to Enable (you need a device connected to YOYORouter to be able to access the settings)

I can't connect to the Wi-Fi network

- Move YOYORouter and the wireless client into the same room, and then test the wireless connection.
- Turn off YOYORouter and the client, then restart it and then turn on the client again.
- Make sure that you have selected the YOYORouter network.
- Make sure you have entered the correct password.
- If the client device needs you to enter authentication and encryption explicitly, enter WPA2 and AES (default YOYORouter settings)
- If WPA2/AWS does not work, try WPA and TKIP (also works with default YOYORouter settings)
- Disable all security settings such as WPA and MAC Address Control. If you are now able to connect, you must re-enable security controls that work with your client.

- Ensure that the LEDs are indicating normally. If not, make sure that the AC power adaptor is connected.
- If you are using other wireless device, home security systems or ceiling fans, lights in your home, your wireless connection may degrade dramatically. Keep your product away from electrical devices that generate RF noise such as microwaves, monitors, electric motors…

My Wi-Fi connection drops or is unreliable

- Position YOYORouter and clients closer together
- Avoid solid walls and other obstructions which reduce the range of the Wi-Fi signal
- Try different antenna orientations for the YOYORouter – stand the device vertically for example.
- Try to keep YOYORouter at least 15cm away from the wall or other objects.
- Try changing the channel on the YOYORouter to avoid interference from other Wi-Fi networks. (By default YOYORouter tries to find a channel with low interference)
- Keep YOYORouter and clients away from electrical devices that generate RF noise, like microwave ovens, audio and TV senders, electric motors, etc.

I have lost the Wi-Fi password

- The default network password is printed on the device label and on the label affixed to the carton in which the device was packaged.

I need to connect a device that does not support WPA or WPA2 /
I want to run YOYORouter in Open or WEP security mode

YOYORouter's default configuration is to accept connection using WPA(TKIP) or WPA2(AES). To change YOYORouter to open or WEP mode:

1. Connect to YOYORouter using a device that does support WPA or WPA2 and enter the WPA password printed on the device's label, or connect using Ethernet.
2. Open the browser at 192.168.1.1,
3. Log in and use the configuration wizard or change settings Advanced > Basic > Wireless > Authentication & Encryption to suit the device that you need to connect.
4. Allow YOYORouter to reboot
5. Reconnect using the new security settings.

I changed the default Wi-Fi password and cannot remember what password I set

- You must reset YOYORouter to factory state.
- Connect using the default network password printed on the device label and on the label affixed to the carton in which the device was packaged
- Open the browser at 192.168.1.1 and log in (password: admin)
- Make any necessary configurations again using the Wizard or the Advanced configuration pages.

I cannot locate the default password for my YOYORouter

The default network password is printed on the device label and on the label affixed to the carton in which the device was packaged. If these labels are missing or damaged:

- Contact YOYOMotion. If possible please supply the MAC address, serial number or IMEI of the device in question.

I am connected to the YOYORouter Wi-Fi network but cannot access the configuration pages

By default the configuration pages are reached by opening the browser on a connected device and selecting 192.168.1.1

- If you previously changed the IP address range, for example to 192.168.123.254, you must use this address to access the configuration pages

- If you changed the IP address and no longer know the new setting, you should perform a factory re-set and then reconfigure your YOYORouter.

5.3. Problems with the Mobile Broadband Connection

YOYORouter isn't connecting to Mobile Broadband

When YOYORouter cannot connect, the indicator is shown. When it flashes, YOYORouter is trying to connect; allow up to 60 seconds to see if the connection attempt is successful. YOYORouter selects a default connection profile, based on the SIM that is inserted.

You can find more information on the status page at 192.168.1.1

Basics:

- Make sure that the SIM is correctly inserted
- If the SIM needs a PIN code, use the configuration wizard to enter the PIN to YOYORouter.
- Check that there is mobile service at your location

The default connection profile suits most users, however you may need to select an alternative:

1. Access the configuration wizard by selecting 192.168.1.1 in your browser
2. At the 3G step, select Manual for Dial-Up Profile
3. Select your country
4. Select your mobile operator. If there are several listings, select the one that most closely corresponds with your subscription (for example, PrePay). If you have special settings or your operator is not shown, select **Others** and enter the details manually.

5. Complete the wizard
6. Allow YOYORouter to restart
7. Check if a connection can now be made.

Note: If you need to ask your mobile operator for settings, you will need the following:

- APN (Access Point Name)*
- Username
- Password
- Primary DNS
- Secondary DNS

* indicates mandatory items. In most cases only APN is needed; DNS is rarely required.

Note: the number to dial is *99#

I have set up my PIN code but YOYORouter still cannot connect

If your SIM has a PIN code, the configuration wizard may not have been able to detect the settings for the mobile operator.

- Restart YOYORouter and re-run the wizard

Or

- Configure YOYORouter manually

My Mobile Internet connection drops unexpectedly

- Position your YOYORouter so that the signal strength is as strong as possible
- Check that the **Connection Control** setting at Advanced > Basic > Network Setup > Connection Control is set to **Auto Reconnect (always-on)**

My Mobile Broadband connection is very slow (2G service)

If the connection is using a 2G network, indicated by

then the very fastest you can expect is around 200kbps download (EDGE) or 54kbps (GPRS).

- Try moving YOYORouter to a window or different location to pick up a 3G signal. (3G network operate at higher frequencies which penetrate buildings less well than 2G)

By default, YOYORouter always selects a 3G network when available (auto mode). It is possible to select 2G only or 3G only service.

- Check that YOYORouter is not in Preferred Service Mode **2G Only** or **2G First;** preferred mode is **Auto Mode.**

Some network operators only provide 3G service for Mobile Broadband devices.

- You must relocate YOYORouter to a position where 3G service is available

My Mobile Broadband connection is very slow (3G service)

A 3G connection is indicated by A strong signal is required to get the best connection speed:

- Try moving YOYORouter to a window or different location to pick up stronger 3G signal.

5.4. Other Problems

I cannot access the wizard – message "Query Status… Please wait a moment…

- You can return to the status screen by using the URL http://192.168.1.1/status.htm?rc=

My analog phone has no dial tone

- There is no mobile service.

My Phone does not display Calling Line Identification (CLI)

- There are many different standards for sending the CLI data to an analog phone. Your phone may not support the CLI signaling used by YOYORouter BE5.

Appendix A Licensing information

This product includes copyrighted third-party software licensed under the terms of the GNU General Public License. Please refer to the GNU General Public License below to check the detailed terms of this license.

The following parts of this product are subject to the GNU GPL, and those software packages are copyright by their respective authors.

Linux-2.6.21 system kernel
busybox_1_00_rc2
bridge-utils 0.9.5
dhcpcd-1.3
ISC DHCP V2 P5
syslogd spread from busybox
wireless tools
ntpclient of NTP client implementation
RT5350 for 802.1X application
GNU Wget

Availability of source code

Please visit our web site or contact us to obtain more information.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply

in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES,
INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS